VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky

BAKALÁŘSKÁ PRÁCE

2010 Jaroslav Šimek

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Bezpečný přenos informací z kamerových systémů

Security transmission of information from camera systems

2010 Jaroslav Šimek

Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 *Studijního a zkušebního řádu pro studium v bakalářských programech* VŠB-TU Ostrava.

Tato práce nemá žádná omezení přístupu

V Ostravě 18. dubna 2010 ……

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 18. dubna 2010 ……

Rád bych na tomto místě poděkoval za oporu své rodině a Ing.Pavlu Nevludovi za kvalitní a přínosné vedení mé práce.

Abstrakt

Téma bakalářské práce „Bezpečný přenos informací z kamerových systémů“ zahrnuje kontinuální sledování vývoje obrazových přenosů, které byly zahájeny převážně na počátku minulého století. Postupně se přenos obrazu zdokonalil díky komunikačním technologiím, které přinesly a také zásadně ovlivnily využití přenosu obrazu mimo rámec televizních přenosů a standardního vysílání. Postupně se začal klást větší důraz na bezpečnost obrazových přenosů a v současné době, kdy v podstatě neexistují žádná omezení ani hranice pro přenos, je díky Internetu posílena role právě oblasti zajištění bezpečného přenosu, který nebude snímán mimo požadovaný cíl. Cílem bakalářské práce je navrhnout optimální a efektivní řešení kamerových systémů použitelných pro podnikatelské subjekty a domácnosti s využitím nejmodernějších prostředků komunikační techniky a se zabezpečením ochrany přenosu v několika možných úrovních. Výsledkem mých teoretických a praktických zkušeností bude návrh zabezpečení přenosu dat dle velikosti a typu subjektu. Zapracovány budou současné možnosti Internetu (WAN, LAN), nástrojů mobilní komunikace (mobilních telefonů), notebooků a snímačů záznamů a zvuků. Návrh bezpečného přenosu dat bude mít navržené 1-3 stupně ochrany a bude optimalizován také ve dvou finančních úrovních (optimální a nejvyšší).

Klíčová slova

přenos obrazu, bezpečný přenos informací, komunikační technologie, nástroje mobilní komunikace, Internet, úrovně bezpečného přenosu, digitální záznam, dohledové pracoviště, digitální kamery, analogové kamery, LAN, WAN

Abstract

The topic of my bachelor's work The Secure Information Transfer from Camera Systems contains a continual observation of the picture transfers development which started mainly at the beginning of the last century. During the course of time, the picture transfer has been improved thanks to communication technologies, which brought the use of picture transfer out of the framework of telecasting and standard broadcasting and had a radical impact on it. Gradually, a greater impact has been put on picture transfer security. Nowadays, when there is virtually no limitation and no boundaries for the transfer, due to the Internet the role of securing the safe transfer has been strengthened. Such transfer shouldn't be read by anybody but the intended target. The goal of my bachelor's work is to design an optimal and effective solution for camera systems usable by businesses and households, which utilizes the latest communication technologies and secures the safe transfer on several levels. The result of my theoretical and practical experience will be the design of a secure data transfer based on the type and size of a subject, which will incorporate the current Internet tools (WAN, LAN), the means of mobile communication (mobile phones), notebooks and records and sounds scanners. The designed secure data transfer will include between 1 and 3 levels of transfer security and will be optimized at two price levels (optimal and the highest).

Key words

picture transfer, secure data transfer, communication technologies, means of mobile communication, Internet, levels of secure transfer, digital record, supervisory workplace, digital cameras, analog cameras, LAN, WAN

Seznam použitých zkratek

AM – Amplitudová modulace – užitečná informace je kódovaná v (amplitudě/síle) nosného signálu, postranní pásma jsou dobře definovatelná

BBC – British Broadcasting Corporation je rozhlasová a televizní společnost plnící funkci veřejnoprávního vysílání ve Velké Británii

CCTV – Uzavřený kamerový systém ke sledování prostor, k zobrazování záběrů z kamer na monitorech

FM – Frekvenční modulace – užitečná informace je kódovaná malými změnami ve frekvenci nosného signálu, postranní pásma jsou teoreticky nekonečná, takže na rozdíl od AM modulace se blízké stanice mohou snáze rušit, na druhou stranu máme k dispozici větší přenosové pásmo a tím i kvalitnější přenos signálu

FTP – File Transfer Protocol znamená v informatice protokol aplikační vrstvy z rodiny TCP/IP. Je určen pro přenos souborů mezi počítači, na kterých mohou běžet rozdílné operační systémy. Jeho podpora je součástí webových prohlížečů nebo specializovaných programů.

FSS – Flying Spot Scanner – snímač běžícím paprskem.

GSM – Globální Systém pro Mobilní komunikaci, původně francouzsky „Groupe Spécial Mobile“ – nejpopulárnější standard pro mobilní telefony na světě.

ICMP – Internet Control Message Protocol je jeden z nejdůležitějších protokolů ze sady protokolů Internetu. Používají ho operační systémy počítačů v síti pro odesílání chybových zpráv, například pro oznámení, že požadovaná služba není dostupná nebo že potřebný počítač nebo router není dosažitelný. ICMP se svým účelem liší od TCP a UDP protokolů tím, že se obvykle nepoužívá síťovými aplikacemi přímo. Výjimkou je např. nástroj ping, který posílá ICMP zprávy „Echo Request“ (a očekává příjem zprávy „Echo Reply“), aby určil, zda je cílový počítač dosažitelný a jak dlouho paketům trvá, než se dostanou k cíli a zpět.

IDS – Intrusion Detection Systém – softwarový bezpečnostní systém.

IP – anglicky Internet Protocol je datový protokol používaný pro přenos dat přes paketové sítě. Tvoří základní protokol dnešního Internetu

IT – Informační technologie

LAN – Local Area Network – lokální počítačová síť.

NAT – Network Address Translation – překlad síťových adres je způsob úpravy síťového provozu přes router přepisem výchozí a/nebo cílové IP adresy, často využíván je i pro změnu čísla TCP/UDP portu u průchozích IP paketů. K tomu patří i změna kontrolního součtu (u IP i TCP/UDP), aby změny byly brány v úvahu. NAT se většinou používá pro přístup více počítačů z lokální sítě na Internet pod jedinou veřejnou adresou. NAT ovšem může způsobit problémy v komunikaci mezi klienty a snížit rychlost přenosu.

NTSC – National Television System(s) Committee je první americká soustava pro přenos barevného televizního signálu, slučitelná s černobílým systémem. Počet řádků v obraze je 455, obrazová frekvence 60 Hz. Úplný signál je rozdělen na jasovou složku a dva rozdílové signály barvy a jasu I a Q, které určují sytost a tón barvy. V soustavě NTSC se současně používají modulace amplitudová, fázová a pro zvuk modulace frekvenční.

PAL – Phase Alternating Line je evropská soustava pro přenos barevného televizního signálu, slučitelná s černobílým systémem, vypracovaná firmou Telefunken v SRN. Počet řádků v obraze je 625, obrazová frekvence 50 Hz a odstup nosného obrazu a zvuku 5,5 MHz. Úplný signál je rozdělen na jasovou složku a dva rozdílové signály barvy a jasu, určující sytost a tón barvy. Jasový kanál má šířku pásma 5 MHz, barvonosný kmitočet je 4,434 MHz. V soustavě PAL se současně používají modulace amplitudová, fázová a pro zvuk frekvenční (kmitočtová). Soustava PAL kombinuje přenosové principy soustavy NTSC a principy soustavy SECAM.

PC – Personal computer – osobní počítač.

Router – Router (směrovač) je v počítačových sítích aktivní síťové zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli. Routování probíhá na třetí vrstvě referenčního modelu ISO/OSI.

RPC – Remote Procedure Call. (vzdálené volání procedur) je technologií dovolující programu vykonat proceduru, která může být uložena na jiném místě, než je umístěn sám volající program. Příkladem může být výpočet funkce na jiném počítači v síti.

RTSP – Real Time Streaming Protocol slouží k doručování obsahu formou datového proudu jednosměrového vysílání (Unicast). Jedná se o protokol na úrovni aplikací, který byl vyvinut speciálně pro řízení doručování dat v reálném čase, např. zvukového obsahu nebo obsahu videa.

SCFM – rezonanční obvod.

SECAM – soustava pro přenos barevného televizního signálu, slučitelná s černobílým systémem, používaná v části východní Evropy. Počet řádků v obraze je 625, obrazová frekvence 50 Hz. Úplný signál je rozdělen na jasovou složku, dvě barevné informace a jeden rozdílový barvonosný signál, který určuje sytost a tón barvy. Jasový kanál má šířku pásma 6 MHz, barvonosné signály mají dvě nosné frekvence 4,250 a 4,406 MHz. V soustavě SECAM se současně používají pro obraz modulace amplitudová a frekvenční, pro zvuk frekvenční.

SSB – Single Side Band (ořezaná amplitudová modulace).

SSTV – Slow-scan Television tj. pomaloběžná televize, televize s pomalým řádkovým rozkladem (dlouhosvitová televize).

UDP – User Datagram Protocol je jedním ze sady protokolů Internetu. O protokolu UDP se říká, že nedává záruky na datagramy, které přenáší mezi počítači v síti. Bývá označován jako nespolehlivý, ale to je označení velmi zavádějící. Na rozdíl od protokolu TCP nezaručuje, zda se přenášený datagram neztratí, zda se nezmění pořadí doručených datagramů nebo zda se některý datagram nedoručí vícekrát. Protokol UDP je vhodný pro nasazení, které vyžaduje jednoduchost nebo pro aplikace pracující systémem otázka-odpověď.

USB – Universal Serial Bus je univerzální sériová sběrnice, která obecně ulehčuje uživateli práci s externími zařízeními připojitelnými k počítači.

WAN – Wide Area Network je počítačová síť, která pokrývá rozlehlé geografické území (například síť, která překračuje hranice města, regionu nebo státu). Největším a nejznámějším příkladem sítě WAN je Internet.

WI-FI – Standard pro lokální bezdrátové sítě (Wireless LAN, WLAN), který vychází ze specifikace IEEE 802.11.

Obsah

1 Úvod…….. **1**

2 Historie přenosu informací z kamerových systémů……. **2**

2.1 Historie oboru všeobecně…..……... 2
2.2 Historie oboru v zahraničí…..…….. 2
2.3 Historie oboru v České republice..……... 3
2.4 Historie snímacích systémů…..…… 4

3 Současné možnosti přenosu informací z kamerových systémů……... **7**

3.1 Digitální kamerový systém s analogovou kamerou…….. 7
3.2 Digitální kamerový systém s digitální kamerou……... 8
3.3 Hybridní digitální kamerový systém……...……. 12
3.4 Ostatní systémy...……. 13

4 Druhy, způsoby a úroveň zabezpečení přenosu…… **14**

4.1 Hardwarové zabezpečení…….. 14
4.2 Softwarové zabezpečení a softwarový firewall…….……... 17
4.3 Software pro vzdálenou plochu……...……. 17
4.4 VPN…….....……. 20
4.5 Zabezpečení přenosu IP kamer..…….. 23

5 Doporučení a optimalizace nastavení zabezpečení přenosu dat dle velikosti a typu subjektu…… **25**

6 Závěr……. **29**

7 Použitá literatura a zdroje…….. **30**

Přílohy…...…… **31**

Seznam obrázků

Obrázek č. 1 Elektromechanický snímač…….…….……. 5
Obrázek č. 2 Schéma CCTV s analogovou kamerou …..……..……. 8
Obrázek č. 3 Schéma CCTV s digitální kamerou ……...….. 9
Obrázek č. 4 Konektor dle standardu IEEE1394…… 10
Obrázek č. 5 Schéma hybridního kamerového systému …… 12
Obrázek č. 6 USB klíčenka…….…..... 12
Obrázek č. 7 Schéma CCTV s digitální kamerou s přenosem v GSM …..…… 13
Obrázek č. 8 HW Firewall od firmy SMC …..……... 14
Obrázek č. 9 SMC přihlašovací okno …..…….. 15
Obrázek č. 10 SMC NAT …..……..…….. 15
Obrázek č. 11 VNC server a klient …..…..…….…... 18
Obrázek č. 12 Radmin klient …..…….. 19
Obrázek č. 13 Náhled na kamerový systém pomocí aplikace Radmin ……. 20
Obrázek č. 14 VPN - možnosti spojení …..……...…… 21
Obrázek č. 15 L2TP tunel …..……..... 22
Obrázek č. 16 PPTP tunel …..……... 22
Obrázek č. 17 IP kamera Vivotek (nastavení hesla)…..…….. 23
Obrázek č. 18 IP kamera Vivotek (nastavení sítě)…..……. 24
Obrázek č. 19 IP kamera Vivotek (náhled live obraz)…..…….. 24
Obrázek č. 20 Nízká úroveň zabezpečení přenosu dat ……. 26
Obrázek č. 21 Střední úroveň zabezpečení přenosu dat …..……. 27
Obrázek č. 22 Vysoká úroveň zabezpečení přenosu dat …..…… 27

1. Úvod

V současné době digitalizace je kladen stále větší důraz na rychlost přenosu informací v jakékoliv podobě, ať již se jedná o obraz, zvuk, data nebo cokoliv dalšího. Zároveň s rychlostí se sledují vysoké nároky na kvalitu a také na finanční náklady přenosů informací. V poslední době se stále více diskutuje o bezpečnosti a ochraně přenosů informací a možnostech zabránění jejich zneužití. Nacházíme se v čase, který nám v podstatě umožňuje realizovat donedávna ještě nepředstavitelné možnosti, nicméně doba opravdové digitalizace a virtuality je stále ještě před námi.

Ve své bakalářské práci jsem se rozhodl zabývat se detailně problematikou bezpečnosti přenosů informací z kamerových systémů. Touto problematikou se již dlouhodobě zabývám ve své dosavadní praxi. Tématu se hodlám věnovat jak ze stránky teoretické, tak také ze stránky praktické.

V první části práce se zaměřím na historii přenosu informací z kamerových systémů. Historie přenosu je mapována od poloviny minulého století a do současné doby zaznamenala opravdu nesrovnatelný pokrok především díky Internetu a jeho možnostem.

Druhá část mé bakalářské práce analyzuje současné možnosti přenosů informací z kamerových systémů. Tyto možnosti analyzuji a hodnotím ve vícekriteriálním modelu a posuzuji jejich silné a slabé stránky ve vazbě na praktickou využitelnost a bezpečnost přenosu. Důraz kladu také na efektivitu řešení po stránce finanční, kterou je v dnešních podmínkách také nutno sledovat a vyhodnocovat poměrem ceny ku přínosu využitého řešení.

Samostatně řeším problematiku samotných způsobů a druhů zabezpečení přenosu dat, které se opírají o využití moderních komunikačních prvků. Postupně také analyzuji, jaké jsou současně dostupné úrovně bezpečnosti a jak je možné každou úroveň zabezpečení využít v praxi tak, aby ve výsledku přinášely optimální řešení dle požadavků a možností jednotlivých uživatelů.

Právě praktická část mé bakalářské práce by měla vyústit v návrh co nejefektivnějšího řešení přenosu informací z kamerových systémů použitelného v současných podmínkách a požadavcích podnikatelských subjektů a také zástupců fyzických osob, jako uživatelů těchto přenosů pro vlastní potřebu.

Všechna mnou navržena řešení efektivního a bezpečného přenosu informací z kamerových systémů budou zahrnovat kritéria, která jsem si vytýčil jako stěžejní, a která jsem ověřil přímo u současných nebo budoucích uživatelů těchto řešení

Moje závěrečné návrhy a řešení budou zahrnovat využití nejmodernějších a zároveň nejefektivnějších postupů pro dané použití s prioritou bezpečného přenosu informací a ochrany přenosu před zneužitím se zapracováním podmínek optimálního ekonomického pořízení a provozu.

2. Historie přenosu informací z kamerových systémů

2.1 Historie oboru všeobecně

Základy zcela prvním přenosům daly na konci 19. století telegrafie po drátě a později telefonie. Těmito způsoby se v podstatě poprvé přenesly určité informace. Následovaly bezdrátové přenosy, které daly vznik oboru radiotechniky, a samotná radiotechnika pak ovlivnila celou řadu jiných oborů, které dnes označujeme jako elektronika a informatika. Popsaný vývoj je v podstatě nejzazší historie prvních přenosů. Radiotechnika jako první umožnila rozvoj sdělování informací zcela novým a jiným způsobem a také stála u počátků možnosti ovlivňovat široké veřejné mínění a také myšlení a názory lidí. Počátkem 30. let minulého století vysílalo již několik stanic s nízkou rozlišovací schopností. Rozlišovací schopnost byla určena počtem řádků v rozsahu středovlnného pásma. Nicméně i při takto problematickém přenosu se vysílání dalo zachytit i na větší vzdálenosti od vysílačů např. v Berlíně, Londýně, Budapešti, Poznani, Vídni nebo Moskvě.

2.2 Historie oboru v zahraničí

Historie televizního přenosu ve světě má své počátky ve dvacátých letech minulého století a jako průkopník je uváděn britský vědec John Logie Baird, který se zabýval vysokofrekvenční technikou. Od roku 1922 se věnoval velmi intenzivně televizní technice na principu rozkladu obrazu, který byl patentován již od konce 19. století. Právě John Logie Baird v lednu 1926 předvedl na poli Královské londýnské společnosti svůj systém nazvaný „televisor“. Pro upřesnění – tento dnes již pravopisně špatně označený název se používal i u nás, ale podle změny pravidel českého pravopisu byl po druhé světové válce upraven název na dnešní používané označení televizor.

Tento původní „televisor“ fungoval na principu, že obraz byl snímán fotobuňkou a elektromechanicky rozkládán pomoci Nipkowova kotouče (patentován v roce 1884 P. G. Nipkowem). Tímto vynálezem a jeho praktickým předvedením také na poli bezdrátového přenosu se zapsal John Logie Baird do historie vývoje společnosti BBC (British Broadcasting Corporation), což byla v té době významná rozhlasová stanice, která mu umožnila využívat svoji techniku pro zkoumání a analýzu dalších možností v přenosu obrazu. Díky této možnosti se mu podařilo v roce 1927 přenést poprvé přes telefonní linky televizní obraz, a to konkrétně z Londýna do Glasgow. O rok později (v roce 1928) se mu podařilo bezdrátově přenést televizní signál přes Atlantik, a to z Londýna do New Yorku.

Vývoj televize pak pokračoval víceméně ve Spojených státech amerických, kde se od roku 1929 realizovaly přenosy barevných obrázků na elektromechanickém principu. Vynález elektronické snímací kamery, kterou představil v roce Philo Tailor Fransworth znamenal další posun v rozvoji přenosu obrazu. V roce 1928 byla vyvinuta snímací elektronka – tzv. „dissektor“, jejž lze považovat za základní prvek nové kamery, která již dokázala plošný obraz elektronicky rozčlenit na jednotlivé body. Tyto kamery se začaly vyrábět průmyslově a dostaly označení „olympijské kamery“, protože právě díky nim se mohly uskutečnit první přenosy z Olympiády konané v roce 1936 v Berlíně.

Další vývoj v oblasti přenosu obrazu přinesl původem Rus Vladimír Kosma Zworykin, který ve své kameře na plně elektronickém principu začal využívat jako snímací elektronku ikonoskop. Toto vylepšení velmi výrazně zvýšilo kvalitu pořízeného obrazu. Ikonoskop byla elektronka, ve které byla

použita metoda snímání jednotlivých bodů obrazu elektronovým paprskem, vychylováným vychylovacími cívkami. Paprsek snímal body obrazu jako náboje ze slídové destičky pokryté rozptýlenými navzájem nespojenými částečkami mozaiky. Destička byla umístěna uvnitř trubice a optikou se na ni vyobrazovala snímaná scéna. Citlivost ikonoskopu byla vysoká.

Ve třicátých letech minulého stolení první televizní stanice vysílaly v rozsahu středovlnného pásma. Pro příjem zvuku se dal použít běžný rozhlasový přijímač, na jehož výstup (reproduktor) byla přes jednoduchý zesilovač připojena doutnavka. Důležitou mechanickou část tvořil Nipkowův kotouč, který prováděl skládání obrazu z jednotlivých přijatých bodů a řádků. Elektromechanická televize se stále zdokonalovala – především tím, že se zvyšoval počet řádků obrazu. Přecházelo se na šedesát, devadesát až na sto dvacet řádků.

Kvalita obrazu se zvyšovala, ale nové přijímače musely být větší a přesněji zhotovené. Zdokonalení obrazu rozkladem na sto osmdesát řádků, které bylo pokusně zavedeno, znamenalo v přijímači použití Nipkowova kotouče o průměru jeden metr při úhlopříčce obrazu dvacet centimetrů. Se zvyšováním počtu řádků v televizním obrazu bylo přenášených bodů příliš mnoho a již nestačila šířka pásma rozhlasových přijímačů. Toto byl důvod, proč se přešlo na rozsahy nad 30 MHz. Ve Francii a v Německu byla od roku 1935 vysílána 180řádková televize s třiceti pěti obrázky za sekundu v pásmu 40 MHz. Obraz měl obvykle rozměr 20 x 26 cm. Současně také došlo k výraznému vylepšení televizních přijímačů, např. Nipkowův kotouč byl nahrazen Braunovou trubicí – obrazovkou s elektrostatickým vychylováním. Přecházelo se postupně od 240řádkového systému na 343 řádků, nejprve v roce 1936 ve Spojených státech amerických a v roce 1938 i v tehdejším Sovětském svazu. Ve Velké Británii se ve třicátých letech používala elektronická televize se 405 řádky, kdy byl obraz i zvuk vysílán amplitudovou modulací. Pravidelné vysílání bylo zahájeno 2. listopadu 1936. Tento způsob vysílání televizního obrazu byl používán až do konce osmdesátých let a ještě v roce 1950 byl mezinárodní komisí považován za nejvhodnější pro používání v celé Evropě. Po skončení druhé světové války bylo televizní vysílání postupně obnovováno. V roce 1946 se definitivně přešlo na televizní obraz s 525 řádky a šedesáti půl-snímky za sekundu. Tento televizní obraz je používán dodnes.

2.3 Historie oboru v České republice

V bývalém Československu již v roce 1935 existovalo kompletní zařízení, které umožňovalo třicetiřádkový televizní obraz. Samotné obnovení televizních přenosů proběhlo u nás až po druhé světové válce a stejně tak tomu bylo i v dalších zemích, kde se z důvodu války televizní přenosy zastavily. Původně byla snaha propojit vývoj v této oblasti mezi Německem a Sovětským svazem za přítomnosti také našich vědců a odborníků, ale tento společný projekt selhal a každá strana vyvíjela a pokračovala v pracích na vývoji černobílých televizních přenosech samostatně. První československé televizní zařízení bylo předvedeno na Mezinárodní výstavě rozhlasu MEVRO v Praze v květnu 1948. Tyto televizní přenosy proběhly v červenci 1948 z XI. Všesokolského sletu. Vysílač s anténními systémy byl umístěn u Petřínské rozhledny a obě stanoviště byla propojena kabelovým spojem. Zkušební vysílání naší Československé Televize bylo oficiálně zahájeno 1. května 1953 a pravidelné vysílání pak začalo od 25. února 1954. Vysílač na Petříně zkonstruovaný v Tesle Strašnice měl výkon 5 kW a pokryl svým signálem Prahu a její okolí. V září roku 1961 dosáhl počet televizních

koncesionářů jednoho milionu, v březnu 1965 dvou milionů, v prosinci 1969 tří milionů a v listopadu 1979 čtyř milionů. Od 9. května 1973 začalo pravidelné vysílání v barvě.

Barevný elektrický přenos a reprodukce pohyblivých viditelných barevných obrazů je logickým pokračováním a zdokonalením televize černobílé. Barva představuje především kvalitativní přínos, rozšířením estetických výrazových prostředků zvětšuje uměleckou hodnotu vytvářených televizních programů. Vlivem rychlého vývoje přešly postupem času všechny televizní stanice na barevné vysílání a ve světě se začaly používat systémy NTSC, SECAM a PAL.

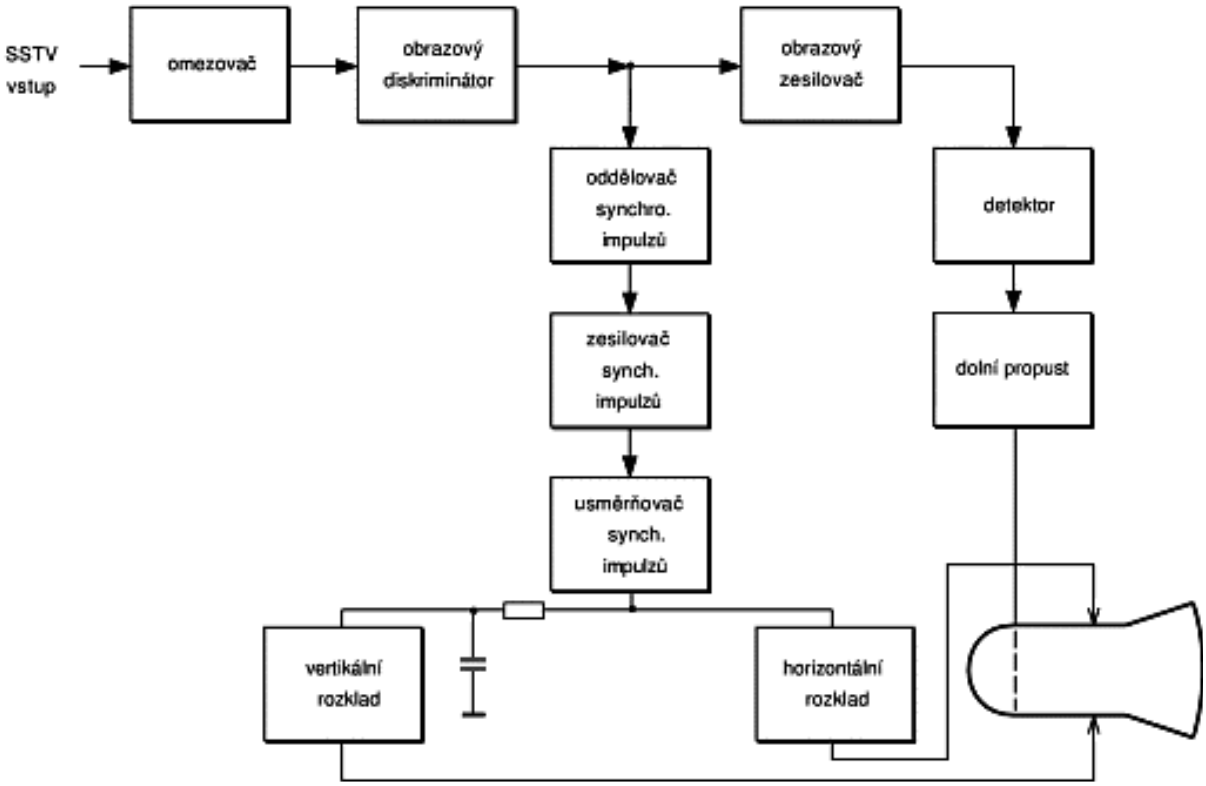
2.4 Historie snímacích systémů

2.4.1 Obrazové monitory SSTV

Na přijímací straně tvoří první článek přenosového řetězce přijímač SSB, AM nebo FM. Z přijímače získaný nízkofrekvenční signál obsahující obrazovou informaci je dále zpracováván obvody obrazového monitoru. Návrh monitoru závisí na druhu vychylovacího systému dlouhodosvitové obrazovky.

Prudký rozvoj různých oborů radiokomunikace vytvořil podněty a možnosti pro bezdrátové přenosy obrazových informací. Základy pro vývoj v této oblasti proběhly u radioamatérů. Příkladem je Copthorne Macdonald, kterému se po mnoha pokusech s amplitudovou a kmitočtovou modulací podařilo vytvořit systém pro přenos obrazové informace s pomalým rozkladem (slow–scan television – SSTV). Brzy na to proběhly úspěšně první transatlantické zkoušky, přičemž přenos nevyžadoval větší šířky pásma, než je zapotřebí k přenosu řeči. Dlouhodosvitový monitor byl také dlouhou dobu nejdůležitějším vybavením pro SSTV přenosy. Tato zařízení nebyla určena jen radioamatérům, ale používala se standardně pro přenos obrazu telefonními linkami.

Blokové schéma monitoru na obr. 1 ukazuje průběh přenosu obrazu. Funguje na principu kmitočtově modulovaného signálu, který kromě obrazové informace obsahuje také synchronizační pulsy. Signál je dále veden přes omezovač, kde je omezen na konstantní amplitudu a jde do obrazového diskriminátoru. Zde obvody videodetekce od obrazového signálu oddělují synchronizační impulzy, které po průchodu diskriminátorem, po zesílení a detekci řídí spouštění vertikálního a horizontálního snímkového rozkladu. Z výstupů těchto obvodů vychází napětí pilovitého průběhu pro vychylovací destičky dlouhodosvitové obrazovky. Signál obrazové informace prochází po oddělení synchronizačních pulsů obrazovým zesilovačem a detektorem. Po filtraci se přivádí na mřížku obrazovky, kde moduluje proud elektronového paprsku a obraz je zobrazován na obrazovce.



Obrázek č. 1 Blokové schéma SSTV monitoru

2.4.2 Elektromechanický snímač

Pro příjem původního osmisekundového SSTV signálu se používalo několika způsobů, které můžeme rozdělit na elektronické a elektomechanické. Mezi čistě elektronické snímací systémy patří kamera, kde je jako snímací prvek použit kvantikon, vidikon nebo jiná snímací elektronka. Dále je to snímač s fotonásobičem pro snímání transparentních nebo netransparentních předloh a *FSS* (*Flying Spot Scanner* – snímač běžícím paprskem). Jako elektromechanický snímač se používal systém podobný FSS, ale pouze pro neprůhledné předlohy, které se snímaly z otáčejícího se válečku. Oproti kameře je jednodušším zařízením snímač FSS, ať už ve své elektromechanické nebo elektronické podobě.

Váleček, na kterém je upevněna snímaná předloha, se otáčí konstantní rychlostí. Každá otáčka odpovídá jednomu obrazovému řádku, který trvá v evropské verzi 60 ms. Pro přenos videosignálu je vyhrazeno 55 ms. Na okraji válečku je upevněn permanentní magnet – podle obvodu válečku odpovídající době 5 ms – sloužící ke generování řádkových synchronizačních impulsů.

2.4.3 Elektronický snímač

Další možností, kterou se signál SSTV získával, je použití snímače s fotonásobičem. Snímač se skládá z prosvětlovací obrazovky, optiky, fotonásobiče, video zesilovače, rozkladových obvodů, obvodu SFCM a synchronizátoru. Synchronizačními a rozkladovými obvody jsou řízeny zesilovače, které aktivuje vychylovací cívky obrazovky. Na obrazovce je vytvořen světelný paprsek, jenž je

snímán objektivem a prosvětluje průhlednou předlohu, např. diapozitiv. Světelný bod se pohybuje a prosvěcuje postupně bod po bodu a řádek po řádku celou předlohu. Světlo procházející předlohou následně dopadá na fotonásobič, na jehož výstupu je elektrické napětí úměrné průhlednosti předlohy. Toto napětí vytváří amplitudově modulovaný obrazový signál, který je pak v patřičných obvodech přeměněn na frekvenčně modulovaný signál SSTV. Tento typ snímače je také možno uspořádat tak, že lze snímat i neprůhledné předlohy, jako třeba fotografie, obrázky na silném papíře, atd. Změna je v tom, že prosvětlovací obrazovka osvětluje přes objektiv předlohu. Světlo, které se od předlohy odráží, je snímáno fotonásobičem a dále zpracováváno SSTV modulátorem.

2.4.4 Vzorkovací kamera

Použití televizní kamery a vzorkovacího převodníku pro snímání SSTV dovoluje vysílat zcela v přímém přenosu a v reálném čase umožňuje i snímání kreseb a nápisů. Všechny snímané objekty musí zůstat po dobu vysílání jednoho snímku nehybné, aby nedošlo k poruše časové spojitosti. To proto, že tyto první kamery prováděly snímání čistě analogovou formou, ne jako pozdější číslicové konvertory, které snímaný obraz převedou na digitální data, uloží v paměti a poté odešlou slow-scan televizní signál. Televizní kamera snímá obraz po řádcích, vzorkovací převodník na svůj vstup z každého řádku, jednoho běhu snímacího paprsku kamery, propouští jen krátký vzorek. Vzorky ze všech řádků rychlé kamery tvoří pak jeden řádek obrazu v normě SSTV. Při dalším běhu snímacího paprsku se poloha vzorkování posune směrem doleva a vytvoří se další řádek SSTV obrazu. Děj se opakuje tak dlouho, dokud není tímto způsobem navzorkován celý obraz. Potom se místo vzorkování přesune zpět doprava a tento proces se podle synchronizačního kmitočtu 50 nebo 60 Hz opakuje každých 7,2 nebo 8 sekund. Vzorkovací převodník se skládá z generátoru řádkového kmitočtu SSTV a současně snímkového kmitočtu TV kamery, obvody pro vytváření vzorkovacích impulsů a generátoru SCFM. Na rozdíl od snímačů FSS, které byly vyráběny pouze v amatérských podmínkách, byly SSTV kamery vyráběny i profesionálně. Amatérská výroba SSTV kamery byla věcí dosti náročnou a použití kamery vyžadovalo téměř studiové nároky pro vysílací stanici, např. správně osvětlení snímané scény.

3. Současné možnosti přenosu informací z kamerových systémů

Bezpečnostní kamery jsou již po několik desetiletí celkem běžnou záležitostí. Dlouhou dobu přenášely obraz jako analogový televizní signál, ale v posledních letech se začaly používat i kamery přenášející obraz digitálně. Rovněž přenos obrazu se po léta neměnil, klasickým médiem zůstává koaxiální kabel. Objevila se řešení využívající bezdrátový analogový přenos obrazu v pásmu 2,4 GHz, a také kamera využívající pro přenos Wi-Fi. V obou případech však přenos obrazu může trpět rušením, kterým zejména ve městech trpí pásmo 2,4 GHz velmi často.

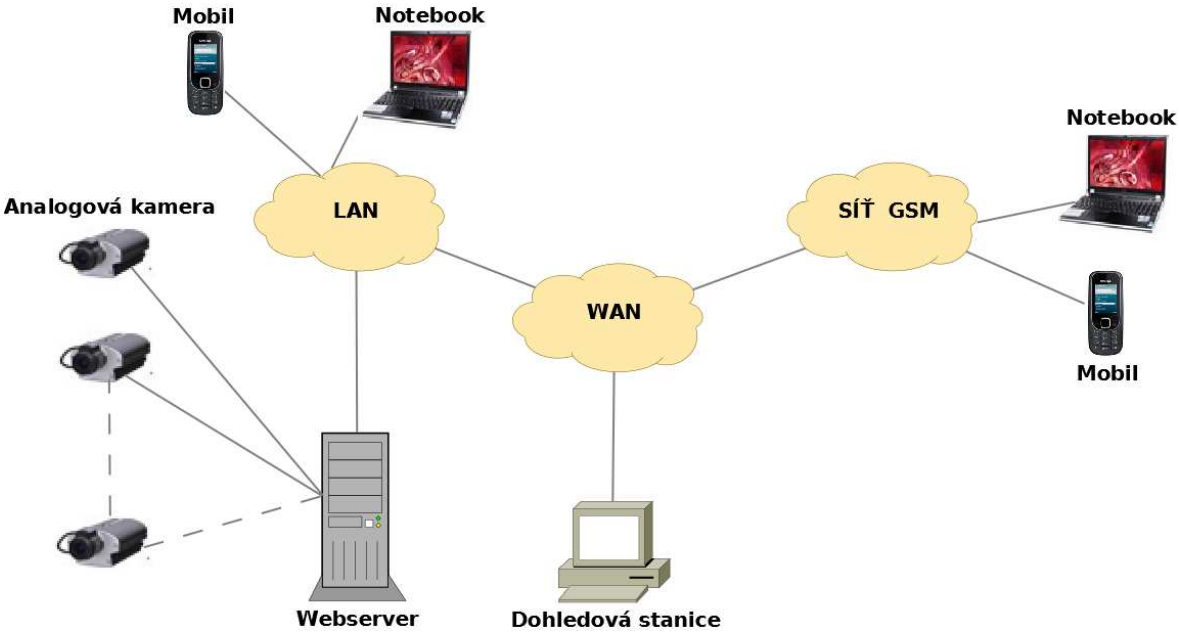
V současné době s rychlým rozvojem technologií existuje mnoho způsobů jak přenášet informace – obraz, zvuk, popřípadě poplach vyvolaný prudkou změnou v obraze (tedy pohybem) z kamerových systémů, respektive z jednotlivých kamer. Je vždy důležité si uvědomit, pro jaký účel byl kamerový systém a jeho dohled vytvořen, a podle toho zvolit způsob zabezpečení těchto informací. Pro záznam je možné používat již zastaralou a v praxi téměř nepoužívanou analogovou technologii se záznamem na magnetický pásek (videokazeta) a pomaloběžný videorekordér, anebo digitální záznam na HDD (hard disk drive). HDD je zařízení, které se používá v počítačích a ve spotřební elektronice k trvalému uchovávání většího množství dat pomocí magnetické indukce a stejně jako flash disk umožňuje uchování dat i při odpojení napájení. Ačkoli je v názvu slovo disk, vlastní médium ve tvaru kotouče není.

Mezi hlavní typy těchto systémů patří:

3.1 Digitální kamerový systém s analogovou kamerou

Analogová kamera je jednosměrný nositel signálu, který končí ve videorekordéru. Po zpracování a úpravě obrazu ze snímače převede obrazovou informaci do analogové formy PAL. Z výstupu kamery je analogový signál veden přenosovým vedením až do místa využití obrazové informace. Typickým využitím obrazu z kamery je jeho uložení v digitálním videorekordéru DVR nebo zobrazení na monitoru stanoviště ostrahy. Obraz je přenášen typicky koaxiálním kabelem s impedancí 75 Ohmů. Jednotlivé typy kabelů se odlišují především průměrem kabelu, mírou útlumu na jednotku délky a také rezistencí na UV záření. Spojení mezi kamerou a monitorem (DVR) je typu bod/bod.

Signál z každé kamery je přenášen nezávislým vedením. Pro přenos lze také použít TWIST převodník, který upravuje signál tak, aby ho bylo možné přenášet po krouceném páru vodičů (nejčastěji UTP kabel). Při využití této technologie lze bez většího zkreslení (rušení) přenášet po jednom kabelu obraz ze dvou kamer. Dále je možné také použít optický video převodník pro přenos po optickém vlákně. Tato alternativa je ovšem finančně značně nerentabilní, když zvážíme dnešní možnosti digitálních kamer.



Obrázek č. 2 Schéma CCTV s analogovou kamerou

Typ kamerového systému, který lze vidět na obrázku č.2, lze k web serveru zabezpečit pouze mechanickými prostředky (krytím, umístěním). Jako web server může být použit digitální rekordér se záznamem na HDD nebo stolní počítač s videokartou (kartami) se vstupy pro analogový signál. Tyto karty jsou nejčastěji se čtyřmi vstupy a do jednoho počítače jich lze umístit až čtyři, pokud to dovolí počet PCI slotů na základní desce. Pro náročnější aplikace jsou již k dispozici COMBO karty, které svou konstrukcí umožňují připojení až šestnácti analogových kamer na jednu kartu. Tato karta také využívá již zmíněný PCI slot.

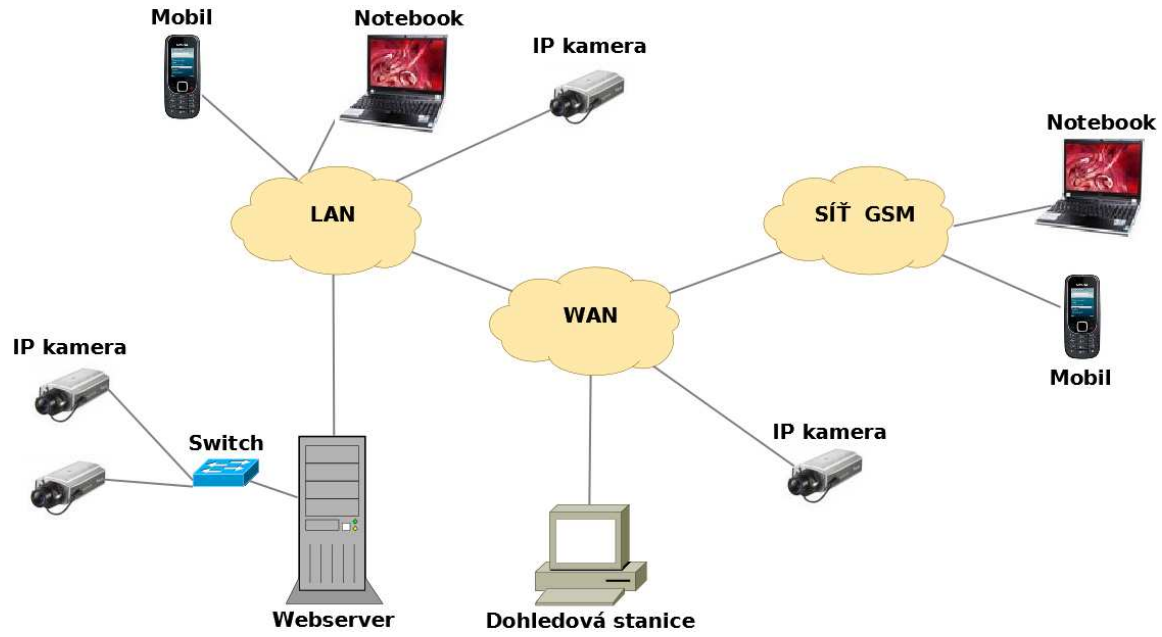
Web servery nám umožňují kvalitní dohled a kontrolu nad kamerovým systémem. Samozřejmě se liší dle výrobce, ale téměř většina těchto systémů nabízí:

- jednoduchou a přehlednou administraci záznamů a uživatelů,
- kvalitu a rychlost záznamu, způsob spuštění záznamu (dle časového plánu, pohybem atd),
- možnost připojení systému do IP sítě,
- dle logů přehled přístupů a jejich selekci do systému v místní síti a Internetu.

3.2 Digitální kamerový systém s digitální kamerou

V uplynulých letech se technologie síťových kamer dostala na úroveň analogových kamer a nyní splňuje stejné požadavky a specifikace. IP kamery dokonce překonávají výkon analogových kamer, protože nabízí řadu užitečných pokročilých funkcí. IP kamera je plně dvousměrná a podporuje tak vytváření vysoce distribuovaných a škálovatelných systémů. Dokáže také komunikovat zároveň s několika aplikacemi, tudíž zvládne vykonávat různé úlohy, jako je detekce pohybu nebo posílání různých video streamů. Lze ji tedy obecně popsat jako kameru a počítač v jednom. Zachycuje a vysílá živé záběry přímo přes IP síť a umožňuje tak autorizovaným uživatelům lokálně nebo na dálku

sledovat, ukládat a spravovat video záběry pomocí standardní síťové infrastruktury založené na IP dle obrázku č. 3.



Obrázek č. 3 Schéma CCTV s digitální kamerou

IP kamera po zpracování a úpravě obrazu dále zachází s obrazem v digitální podobě. Kvůli enormně vysokým nárokům na šířku pásma potřebného pro přenos neupraveného digitálního obrazu je před odesláním obrazových dat z kamery obraz komprimován použitím ztrátové komprese například ve formátu MPEG4. Zkomprimovaný digitální signál je pak přenášen po krouceném čtyřpárovém vodiči ve standardu počítačové sítě Ethernet. Oproti přenosu signálu z analogové kamery vyžaduje tento způsob samostatné vedení jen do nejbližšího aktivního síťového prvku sítě Ethernet. Dále je signál přenášen po vedení souběžně s ostatními daty.

Zásadní výhodou přenosu signálu digitální formou je skutečnost, že signál ani na velké vzdálenosti kvalitativně nedegraduje. Jeho kvalita je stále stejná. Tato skutečnost umožňuje díky IP systémům vybudovat kamerové systémy většího rozsahu i komplexnosti, než jsou systémy analogové. Při více požadavcích na kamerový systém IP přináší úsporu času a nákladů při instalaci.

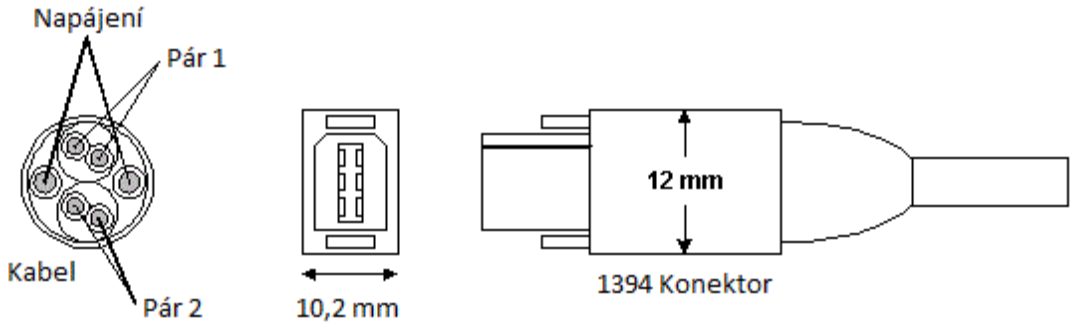
Známe dva základní druhy web kamer:

1. **Obyčejná web kamera** potřebuje připojení k počítači kabelem většinou nepřesahujícím délku 3 m přes USB port nebo IEEE1394 a hlavně vyžaduje ke svému fungování zapnutý počítač.

USB 2.0 neboli Universal Serial Bus, je rozhraní prosazované především (ale nejenom) firmami Intel a Microsoft. Jedná se o sériové rozhraní s rychlostí přenosu dat maximálně 480 Mbps (megabitů za sekundu), určené, zhruba řečeno, k připojování všech zařízení, která se dají stejně snadno připojit přes

rozhraní SCSI (Small Computer System Interface), což je standardní rozhraní a sada příkazů pro výměnu dat mezi externími nebo interními počítačovými zařízeními a počítačovou sběrnicí.

IEEE1394 neboli rozhraní FireWire vytvořila firma Apple jako levné, ale přitom výkonné rozhraní, umožňující nejen propojování počítačů a nejrůznějších periférií, ale i jednotlivých zařízení domácí elektroniky. Rozhraní FireWire je navrženo natolik flexibilně, že může stejně dobře sloužit pro připojení pevného disku k počítači, jako pro propojení digitálního videopřehrávače s digitálním televizorem – a tak vytvořit dosud neexistující standard i zde. Vzhledem k výhodám, které rozhraní FireWire nabízí, jej 12. prosince 1995 přijalo IEEE (Institute of Electrical and Electronic Engineers) jako standard IEEE1394. Ačkoli se jedná o zcela univerzální systém, umožňující jak asynchronní, tak i isochronní přenos, stává se dnes zvláště zajímavým v souvislosti s nástupem digitálního videa. Rozhraní totiž nabízí dostatečné prostředky pro přenos a zpracování dat, reprezentujících videosekvence, jak mezi klasickými koncovými zařízeními (kamera, videopřehrávač, monitor) navzájem, tak i mezi nimi a počítačem (kde pak máme prakticky neomezené možnosti zpracování snímků). Vlastní přenosová rychlost kabelu není pevně určena; stávající podoba normy počítá s jednou ze tří přenosových rychlostí, a to 100, 200 nebo 400 Mbps, a pracuje se na rozšíření pro ještě vyšší přenosové rychlosti (řádu Gbps a více). Norma IEEE1394 definuje tři nejnižší úrovně síťového modelu ISO/OSI: transakční, linkovou a fyzickou. Na nejvyšší, transakční úrovni je zabezpečeno předávání asynchronních paketů prostřednictvím protokolu, odpovídajícího normě ISO/IEC 13213 (read/write/lock). Linková úroveň zabezpečuje předávání datagramů a řízení isochronního přenosu. Konečně na fyzické úrovni jsou definovány mechanismy, zabezpečující inicializaci sběrnice, její synchronizaci (tj. zabezpečení toho, aby v jednom okamžiku vysílal data pouze jediný uzel) a konečně i fyzické provedení kabelů a konektorů.



Obrázek č. 4 Konektor dle standardu IEEE1394

Jak vidíme na obrázku č. 4, kabel přenáší kromě vlastních dat také napájení. To je důležité z několika důvodů: předně, linkové obvody mohou být napájeny i v případě, že je zařízení jako celek odpojeno od sítě; díky tomu síť IEEE1394 pracuje korektně i tehdy, jsou-li zapojena jen některá z jejích zařízení. U přístrojů s uzemněním mohou být linkové obvody – napájené z kabelu – galvanicky odděleny od ostatní elektroniky, čímž se zabrání vzniku zemních smyček. Konečně, jednoduchá zařízení s nevelkou spotřebou proudu (typicky např. kamery nebo mikrofony) mohou být napájena přímo z kabelu, a nepotřebují tedy samostatný síťový přívod nebo baterie, což dále zjednodušuje

zapojení sítě. V principu může být rozhraním IEEE1394 vybaveno jakékoli zařízení, které si má vyměňovat data s jiným (a/nebo které má být řízeno odjinud, případně má samo řídit jiné). V praxi se zřejmě v nejbližší době budeme moci setkat s videokamerami vybavenými rozhraním IEEE1394 (zde se rozhraní obvykle nazývá DV nebo i.Link) a s kartami do počítače, reprezentujícími bridge mezi sběrnicí IEEE1394 a sběrnicí počítače.

2. **IP kamera** má svou vlastní IP adresu, je připojitelná k síti a má vestavěný webový server, popřípadě FTP server, FTP klienta, e-mailového klienta, správu alarmů, programovatelnost a mnoho dalších funkcí. Tyto IP kamery nemusí být připojeny k počítači, mohou fungovat nezávisle a můžeme je umístit kamkoli, kde máme připojení k IP síti.

Hlavní výhody IP kamer jsou:

- jednoduchá instalace a pružnost – lze je umístit kdekoliv, kde je dostupná IP síť,
- vše potřebné pro vysílání video záběrů přes síť je již v kameře,
- vysoká kvalita obrazu, díky standardnímu formátu JPEG a MPEG kompresi.

JPEG (Joint Photographic Experts Group) je standardní metoda ztrátové komprese používané pro ukládání počítačových obrázků ve fotorealistické kvalitě.

MPEG (Motion Picture Experts Group), v překladu „skupina expertů pro pohyblivý obraz“, což je název skupiny standardů používaných na kódování audiovizuálních informací (např. film, obraz, hudba) pomocí digitálního kompresního algoritmu.

Možnosti záznamu z kamerových systémů

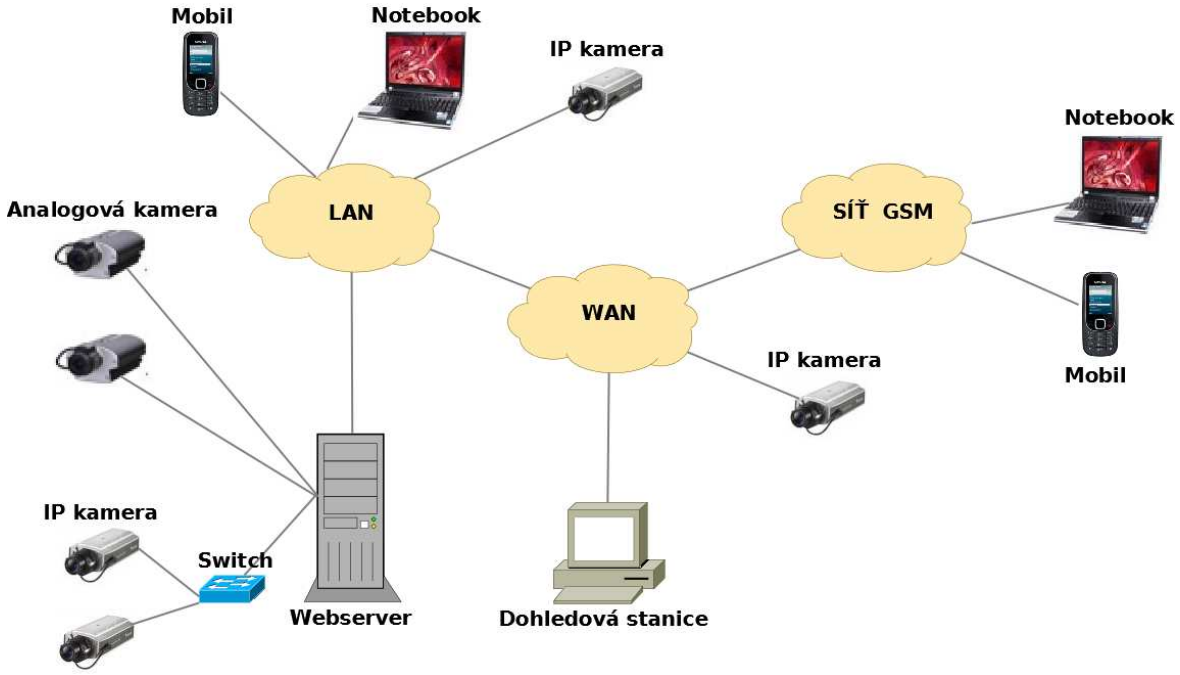
První metoda záznamu obrázků je velmi prostá. Využívá nějakého FTP serveru dostupného kameře. To může být třeba FTP server Vašeho poskytovatele připojení k Internetu, který bývá zpravidla zdarma. Tato metoda není ovšem příliš bezpečná, protože heslo a uživatelské jméno k FTP serveru se přenáší po Internetu nezabezpečené. Dále je potřeba si uvědomit, že tato varianta je zajímavá pouze pro zákazníky, kteří neplatí za připojení podle objemu dat nebo času připojení. Dalším negativem je nepřehlednost uložených dat – při pohledu na FTP server bude v každé složce velké množství obrázků a najít mezi nimi ten pravý není zrovna jednoduché.

Druhá metoda záznamu obrázků využívá FTP serveru uvnitř domácí sítě. Tento FTP server může být realizován na některém dostupném PC v síti. Je to levné řešení archivace záznamu na vlastním hardware a zabezpečení je na stejné úrovni jako v celé místní síti. Jediným negativem je nepřehlednost při práci s FTP serverem, ta byla popsána výše.

Třetí metoda je náročnější, vyžaduje totiž počítač, který bude běžet 24 hodin denně. Software je podle typu video karty (popřípadě kamery) dodáván výrobcem, takže na něj není potřeba vynakládat další

finanční prostředky. Tento způsob umožňuje záznam videa na disk počítače, a to včetně zvuku a událostí. Počítač pak stahuje video z kamery a ukládá jej do databáze. Díky ní je hledání událostí a časů velmi zjednodušené a celkem přehledné.

3.3 Hybridní digitální kamerový systém



Obrázek č. 5 Schéma hybridního kamerového systému

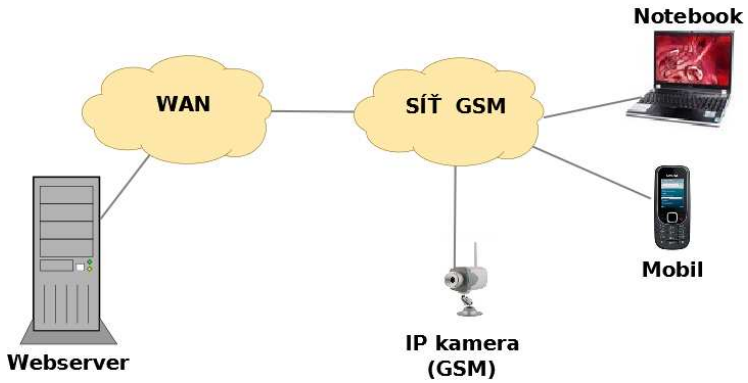
Z obrázku č. 5 lze vyčíst, že tento systém využívá spojení obou systémů popisovaných v předcházejících kapitolách, a to díky DVR a PC kartám (popřípadě COMBO karty), které umožňují připojení analogových i digitálních kamer současně do jedné komplexní infrastruktury. Při pořízení takového systému, kdy není z hardwarového hlediska možné další rozšíření, je alternativa použití IP kamer dobrým východiskem. Rozšíření takových systémů o další IP kamery je většinou ošetřeno pořízením licence na určitý počet těchto kamer a tato licence je uložená v HW klíči.

Obrázek č. 6 USB klíčenka

HW klíč (hardwarový klíč) je fyzický prostředek ochrany programu proti nelegálnímu používání. V dnešní době se nejčastěji objevuje v podobě malé USB klíčenky – viz obrázek č. 6. Hardwarový klíč obsahuje uvnitř ochranné elektrické obvody, které vytvářejí kód, bez něhož takto chráněný program nebude fungovat. Mohou také obsahovat kód pro dešifrování části programu apod.

3.4 Ostatní systémy

Jako další možnost digitálních kamerových systémů lze využít kompaktní mobilní dohledový a monitorovací systém, zobrazený na obrázku č. 7, pro přenos videa s vysokým rozlišením a jednotlivých obrázků přes GPRS/EDGE sítě mobilních operátorů.



Obrázek č. 7 Schéma CCTV s digitální kamerou s přenosem v GSM

Tento systém je využitelný pro vzdálený bezdrátový přenos nebo na místech, kde není možnost připojení k Internetu. Je ideální pro dohled na dočasných aplikacích (např. stavbách, montážích a venkovních kulturních akcí), vzdálených místech nebo pohybujících se objektech (např. kontrola mobilního majetku), ale bez problémů zastane i potřeby dlouhodobého nasazení tam, kde nechceme investovat do náročných stavebních úprav nebo místní kabeláže. Video nebo jednotlivé obrázky, popř. sekvence obrázků lze zasílat pomocí sítě GSM na předem definovaná mobilní čísla, popřípadě web servery. Pro minimalizaci toku dat se zde používá komprese JPEG a MPEG-4. Dále lze ukládat záznamy na mikroSD kartu. Konfigurace se u těchto systémů provádí pomocí interního web serveru, SMS zprávami a nebo pomocí USB kabelu.

4. Druhy, způsoby a úroveň zabezpečení přenosu

4.1 Hardwarové zabezpečení

Hardwarovým zabezpečením je myšleno zabezpečení kabeláže (krytím, snížením dostupnosti) u analogových systémů, kde video signál od snímací kamery k video serveru není vůbec upravován nebo šifrován. Dále je možné k video serverům používajícím IP kamery doplnění samostatné síťové karty, která bude určena pouze pro podsíť těchto kamer a dálkové zpřístupnění a administrace systému bude zprostředkována v jiné podsíti, kde téměř všechny dostupné video servery již obsahují nějakou metodu ochrany, jako jsou:

- Autentizace uživatele
- Práva uživatele
- Filtrování povolených IP adres (white a black list)
- Šifrování v podobě software k vzdálené správě

Patří sem také hardwarový firewall, jako je například na obrázku č. 8, kterým můžeme doplnit jakýkoliv systém využívající LAN sítě pro vzdálenou komunikaci.

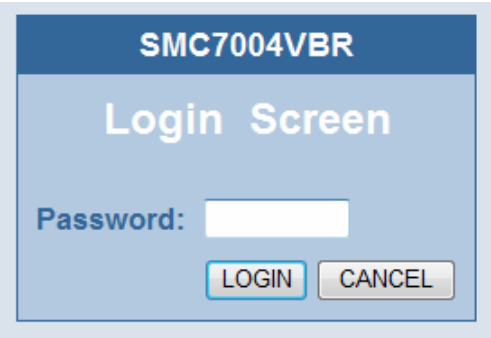
Obrázek č. 8 HW Firewall od firmy SMC

Firewall je síťové zařízení, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říci, že slouží jako kontrolní bod, který definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Tato pravidla historicky vždy zahrnovala identifikaci zdroje a cíle dat (zdrojovou a cílovou IP adresu) a zdrojový a cílový port, což je však pro dnešní firewally už poměrně nedostatečné. Modernější firewally se opírají přinejmenším o informace o stavu spojení, znalost kontrolovaných protokolů a případně prvky IDS. Firewally se během svého vývoje řadily zhruba do následujících kategorií:

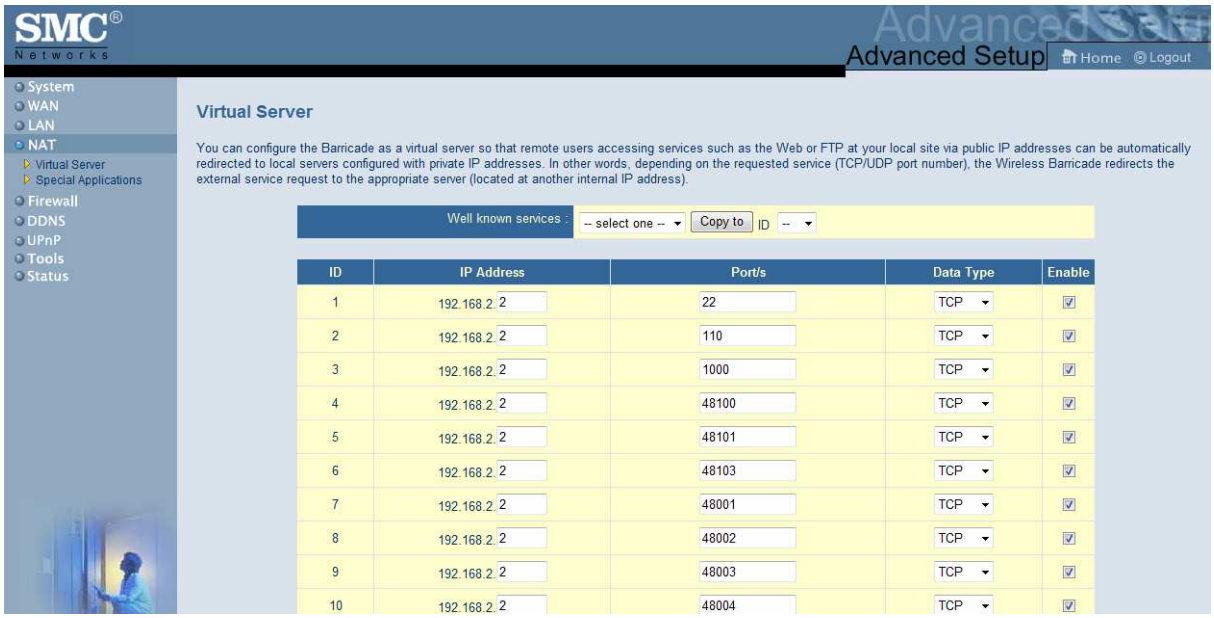
- Paketové filtry
- Aplikační brány
- Stavové paketové filtry
- Stavové paketové filtry s kontrolou známých protokolů a popř. kombinované s IDS

Pro názornou ukázku zde uvádím náhled pro práci s HW firewallem od firmy SMC. Na obrázku č. 9 je patrné, že před samotnou konfigurací je nutné přihlásit se oprávněným heslem. Uživatel zde může přehledně a snadno nastavovat mnoho parametrů, jako je konfigurace firewallu, filtrování IP adres,

povolení otevřených portů s typy přenosových protokolů (obrázek č. 10), a tím vším zkvalitnit ochranu své vnitřní sítě. Samozřejmostí je přehledný log, kde lze nalézt jak přihlášení ke konfiguraci, tak i komunikaci přes toto zařízení jednak povolenou, tak i zakázanou.



Obrázek č. 9 SMC přihlašovací okno



Obrázek č. 10 SMC NAT

Paketové filtry

Nejjednodušší a nejstarší forma filtrování, která obsahuje pravidla definující z jaké adresy a portu na jakou adresu a port může být doručen procházející paket., Kontrola se provádí na třetí a čtvrté vrstvě modelu síťové komunikace. Výhodou tohoto řešení je vysoká rychlost zpracování dat, proto se ještě i dnes používají na místech, kde není potřebná přesnost nebo důkladnější analýza procházejících dat, ale spíš jde o přenosy vysokorychlostní. Nevýhodou je nízká úroveň kontroly procházejících spojení, která zejména u složitějších protokolů (např. FTP, RPC apod.) nejen nedostačuje ke kontrole vlastního spojení, ale pro umožnění takového spojení vyžaduje otevřít i porty a směry spojení, které mohou být využity jinými protokoly, než bezpečnostní správce zamýšlel povolit. Mezi typické

představitele paketových filtrů patří např. tzv. ACL (Access Control Lists) ve starších verzích operačního systému IOS na routerech spol. Cisco Systems, popř. starší varianty firewallu v linuxovém jádře.

Aplikační brány (někdy také Proxy firewally)

Veškerá komunikace přes aplikační bránu probíhá formou dvou spojení – klient (iniciátor spojení) se připojí na aplikační bránu (proxy), ta příchozí spojení zpracuje a na základě požadavku klienta otevře nové spojení k serveru, kde klientem je aplikační brána. Data, která aplikační brána dostane od serveru, pak zase v původním spojení předá klientovi. Kontrola se provádí na sedmé (aplikační) vrstvě síťového modelu OSI (proto se těmto firewallům říká aplikační brány).

Jedním z vedlejších efektů použití aplikační brány je, že server nevidí zdrojovou adresu klienta, který je původcem požadavku, ale jako zdroj požadavku je uvedena vnější adresa aplikační brány. Aplikační brány díky tomu automaticky působí jako nástroje pro překlad adres (NAT), nicméně tuto funkcionalitu má i většina paketových filtrů.

Výhodou tohoto řešení je poměrně vysoké zabezpečení známých protokolů.

Nevýhodou je zejména vysoká náročnost na použitý HW – aplikační brány jsou schopny zpracovat mnohonásobně nižší množství spojení a rychlosti, než paketové filtry a mají mnohem vyšší latenci. Každý protokol vyžaduje napsání specializované proxy, nebo využití tzv. generické proxy, která ale není o nic bezpečnější, než využití paketového filtru. Většina aplikačních bran proto uměla kontrolovat jen několik málo protokolů (obyčejně kolem deseti). Původní aplikační brány navíc vyžadovaly, aby klient uměl s bránou komunikovat a neuměly dost dobře chránit svůj vlastní operační systém. Tyto nedostatky se postupně odstraňovaly, ale po nástupu stavových paketových filtrů se vývoj většiny aplikačních bran postupně zastavil. Přeživší se dnes používají už jen ve velmi specializovaných nasazeních.

Typickými představiteli aplikačních bran byly např. The Firewall Toolkit a z něj vycházející Gauntlet spol. TIS později zakoupený společností NAI.

Stavové paketové filtry

Stavové paketové filtry provádějí kontrolu stejně jako jednoduché paketové filtry, navíc si však ukládají informace o povolených spojeních, které pak mohou využít při rozhodování o tom, zda procházející pakety patří do již povoleného spojení a mohou být propuštěny, nebo zda musí znovu projít rozhodovacím procesem. To má dvě výhody. Jednak se tak urychluje zpracování paketů již povolených spojení, jednak lze v pravidlech pro firewall uvádět jen směr navázání spojení a firewall bude samostatně schopen povolit i odpovědní pakety a u známých protokolů i další spojení, která daný protokol používá. Například pro FTP tedy stačí nastavit pravidlo, ve kterém povolíte klientovi připojení na server pomocí tohoto protokolu. Protože se jedná o známý protokol, firewall sám povolí navázání řídícího spojení od klienta na port 21 serveru, odpovědi serveru na klientem použitý zdrojový port a po příkazu, který vyžaduje přenos dat, povolí navázání datového spojení z portu 20

serveru na klienta na port, který si klient se serverem dohodli v rámci řídícího spojení a pochopitelně i odpovědní pakety z klienta zpět na port 20 serveru. Zásadním vylepšením je i možnost vytváření tzv. virtuálního stavu spojení pro bezstavové protokoly, jako např. UDP a ICMP.

K největším výhodám stavových paketových filtrů patří jejich vysoká rychlost, poměrně slušná úroveň zabezpečení a ve srovnání s výše zmíněnými aplikačními branami a jednoduchými paketovými filtry řádově mnohonásobně snazší konfigurace. Díky zjednodušení konfigurace pak také nižší pravděpodobnost chybného nastavení pravidel obsluhou.

Nevýhodou je obecně nižší bezpečnost, než poskytují aplikační brány.

Typickými představiteli této kategorie firewallů jsou např. FireWall-1 spol. Check Point do verze 4.0, starší verze Cisco PIX, Cisco IOS Firewall, starší verze firewallů Netscreen spol. Juniper a z volně dostupných produktů iptables v linuxovém jádře a ipfw v BSD (Berkeley Software Distribution, též Berkeley Unix).

4.2 Softwarové zabezpečení a softwarový firewall

Téměř každý výrobce poskytuje software k dodávanému kamerovému systému pro jeho snadnou obsluhu a kompletní dálkovou správu. V praxi lze potom definovat, zda bude systém vzdáleně dostupný jen pomocí těchto softwarů, anebo i jakéhokoliv Internetového prohlížeče a i zde jsou případy, kdy je podporován výhradně prohlížeč od firmy Microsoft. Tyto softwary obsahují kodeky, bez kterých je vzdálené sledování nemožné. Při prvním připojení do systému – po autentizaci uživatele a kontroly jeho práv – se do vzdáleného klienta nahraje z video serveru zásuvný plugin do internetového prohlížeče (prvek ActiveX), který potom umožní další práci s tímto systémem. Aby bylo možné vůbec pracovat s těmito systémy vzdáleně, je nutné mít veřejnou IP adresu a nastavit, resp. povolit parametry jako jsou například:

- Typ přenosového protokolu
- NAT
- IP adresa web serveru popřípadě klienta
- Brána firewall

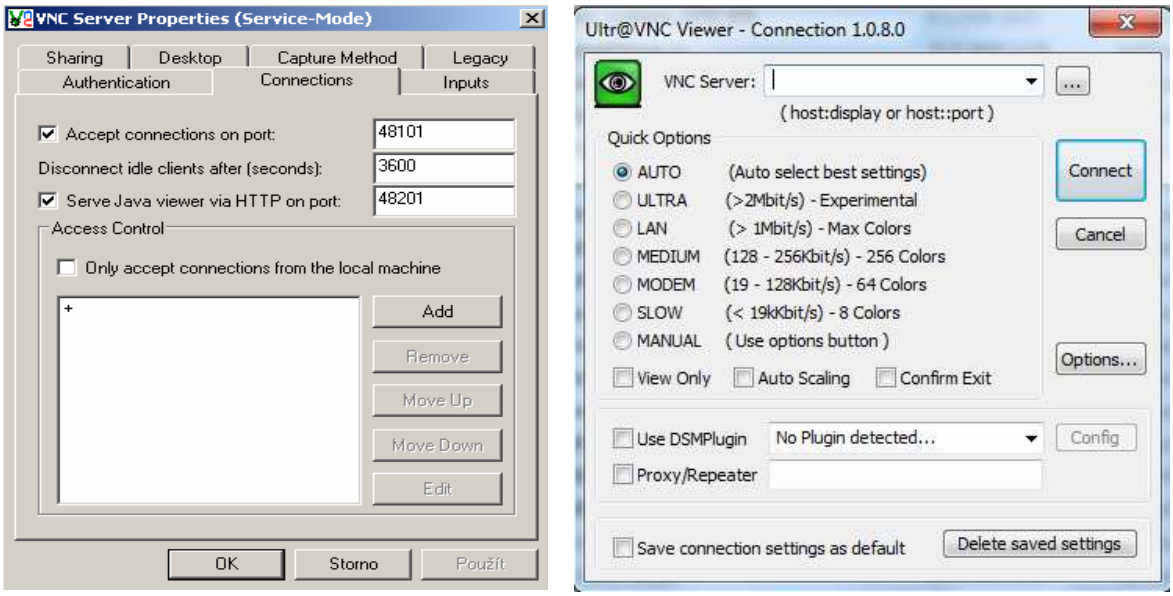
Tyto parametry se liší dle výrobce a také komfort pro uživatele je různý. Některé systémy i v dnešní moderní době ještě dost zaostávají za našimi představami, a proto je důležité si při výběru kamerového systému zvolit priority a požadavky, co od systému chceme a hlavně očekáváme. Dále lze systém web serveru, který funguje na operačním systému (nejčastěji Windows), doplnit softwarovým firewallem anebo využít jeho vlastní.

4.3 Software pro vzdálenou plochu

Pro ukázku jsem si vybral dva, a to **VNC a Radmin**

Virtual Network Computing (VNC) je grafický program (viz obrázek č. 11), který umožňuje vzdálené připojení ke grafickému uživatelskému rozhraní pomocí počítačové sítě. VNC pracuje jako klient-server, kde server vytváří grafickou plochu v operační paměti počítače a komunikuje přes síť s klientem, který plochu zobrazuje uživateli (většinou na jiném počítači). Pro komunikaci se používá

protokol RFB, jehož cílem je minimalizovat objem přenášených dat mezi klientem a serverem a umožnit tak komunikaci i přes pomalejší datové linky (např. přes Internet).



Obrázek č. 11 VNC server a klient

Kompletní VNC systém se skládá z klienta, serveru a komunikačního protokolu. VNC server je program, který sdílí svoji obrazovku. VNC klient (viewer) je program, který zobrazuje sdílenou plochu a ovládá server. VNC protokol (RFB) používá bitmapové řešení, kde každý pixel má své souřadnice, kde plocha se bere jako jeden obrázek, na který se malují objekty, a jako celek se pak pošle klientovi. Přenášejí se pouze změny (například pohyb myši, psaní textu, zobrazování videa). V praxi pohneme kurzorem, server si přebere souřadnice, a na hostitelském počítači se provede pohyb kurzoru, který se pak zpětně promítne do klienta.

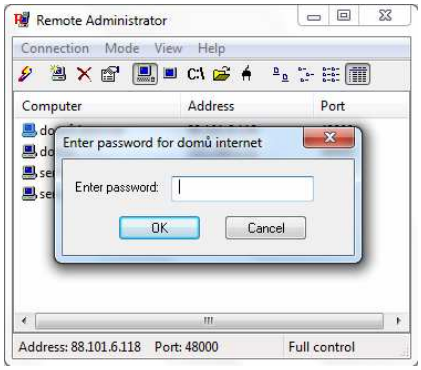
VNC standardně používá TCP porty 5900 až 5906. Každý port koresponduje s jednotlivými obrazovkami. V mnoha implementacích (např. RealVNC) je dostupný Java prohlížeč na portech 5800 až 5806, umožňující klientům ovládání mimo jiné i přes webový prohlížeč podporující Javu. Ostatní porty mohou být použity, pokud jsou klient i server patřičně zkonfigurovány. Použití VNC přes Internet funguje dobře, pokud je na obou koncích širokopásmové připojení. Nicméně někdy je třeba pokročilá konfigurace NAT, firewalu a routeru, aby spojení bezproblémově prošlo skrz toto nastavení. Komunikace mezi klientem a serverem standardně zabezpečena není. Samotná autentizace je poměrně bezpečná, protože se pro ověření hesla používá systém challenge-response (náhodná výzva a kontrolovaná odpověď), takže heslo neputuje po síti v nezašifrované podobě (je omezen útok Teplat attack). Po autentizaci můžeme pracovat se vzdálenou plochou a daty, v našem případě s kamerovým systémem, ale síťový provoz mezi klientem a serverem už zašifrován není, a veškerá komunikace tedy může být odposlouchávána (a rekonstruován nejen obsah obrazovky, ale zachyceny i všechny pohyby myši a stisky kláves, tj. útok Man in the middle). Proto se doporučuje VNC relaci

navázat skrz zabezpečený tunel (SSH, VPN) nebo použít doplňující moduly, které umožňují automaticky veškerou komunikaci zašifrovat.

Dalším a bezpečnějším pomocníkem pro vzdálenou správu systémů, který je vidět na obrázku č. 12 je aplikace **Radmin**. Je to světově známá, oceněním vyznamenaná aplikace pro zabezpečené ovládání vzdáleného přístupu, která umožní práci na vzdáleném počítači v reálném čase, jako by byl ovládán přímo klávesnicí a myší z připojeného lokálního počítače. Tato aplikace je ideálním řešením pro vzdálený přístup. Výkonnost aplikace Radmin předčí všechny ostatní aplikace s ohledem na rychlost, spolehlivost a zabezpečení! Podporuje operační systémy Windows 7/Vista/XP/2008/2003/2000 (32-bit, 64-bit).

S tímto programem lze provést správu malých, středních a velkých sítí LAN/WAN vzdáleným přístupem. Pomocí aplikace Radmin lze v případě potřeby služeb administrátora uspořit čas a peníze pomocí vzdáleného přístupu k počítačům z libovolného místa a tím pádem i efektivně a bezpečně nakládat s daty z kamerových systémů. Zabezpečení je bezpodmínečně nutné pro jakoukoliv aplikaci vzdáleného přístupu, přičemž tato aplikace patří k těm nejvíce zabezpečeným pro vzdálený přístup. Po spuštění klienta si zvolíme režim přenosu dat a po přihlášení oprávněným heslem můžeme systém vzdáleně ovládat v těchto režimech:

- plná kontrola nad vzdálenou plochou
- sledování plochy bez možnosti ovládání
- telnet nebo přenos souborů
- vypnutí, restart stanice, serveru



Obrázek č. 12 Radmin klient

Nejdůležitější funkce zabezpečení zahrnují:

- Moderní 256bitové AES výkonné šifrování všech toků dat.
- Možnost volby mezi zabezpečením Windows nebo zabezpečením Radmin.
- Zabezpečení Radmin podporuje různé druhy povolení pro uživatele, dodatečně zapsané do seznamu přístupových oprávnění Radmin Server. Aplikace Radmin využívá výměnu klíčů spočívající na Diffie-Hellmanovu algoritmu s velikostí klíče o 2048 bitů.
- IP filtr povoluje přístup k aplikaci Radmin Server pouze z určitých IP adres a sítí.
- DNS název a jméno uživatele se přidává do protokolového souboru.
- Důmyslná ochrana na základě hádání hesla.

Po autentizaci již můžeme bezpečně pracovat se vzdálenou plochou a daty, v našem případě s kamerovým systémem.

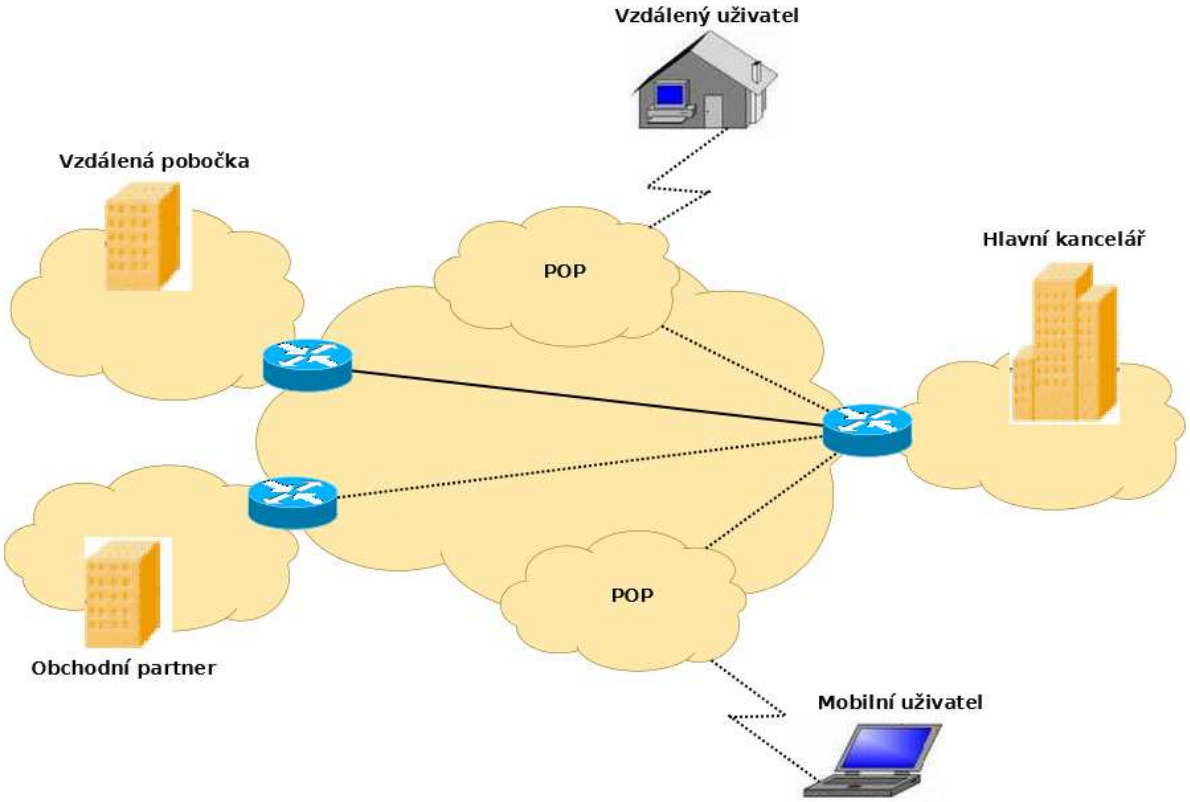
Obrázek č. 13 Náhled na kamerový systém pomocí aplikace Radmin

Při použití Radmin security lze nastavit různá povolení pro jednotlivé uživatele Radminu. K autentikaci uživatele a nastavení klíče přístupu se používá výměna dat dle upraveného Diffie-Hellmanova algoritmu s klíčem o velikosti 2048 bitů. Radmin je vybaven integrovaným obranným mechanismem testování kódu, který zabraňuje provedení úprav kódu aplikace a pro každé připojení generuje jedinečné soukromé klíče pomocí aplikace dlouhé sekvence náhodných bitů, která vytváří neprůlomnou ochranu. Přístupové heslo je uloženo v zašifrované podobě a nikdy se nepřenáší mezi počítači jakoukoliv formou, což zabraňuje třetím stranám v získání nebo vytváření klíčů. Radmin server chrání aktivně všechna nastavení, která jsou uložena v registru systému, a spouští se jako služba a ne jako aplikace v operačním systému, což podporuje zdokonalení zabezpečení.

4.4 VPN

Celý anglický název zní Virtual Private Network neboli česky privátní síť. VPN slouží k připojení z nedůvěryhodné sítě (což je vlastně veřejná síť Internet) do privátní sítě např. firemní, školní či domácí. Pomocí tohoto způsobu připojení můžeme dosáhnout, že tímto způsobem spojené počítače budou spolu komunikovat, jako by byly ve společné privátní síti. Komunikace je šifrovaná a autentizovaná. Proto je tento způsob bezpečný pro přenos kamerového systému. Existuje několik druhů spojení:

- LAN-LAN – toto spojení se využívá mezi LAN sítěmi. Po tomto způsobu sáhnou firmy, které mají více poboček a chtěly by mít svůj intranet. Aby bylo možné toto spojení realizovat, musí se vytvořit na směrovačích tunel bod-bod.
- Klient-Klient – toto připojení se v praxi málokdy objevuje. Každý z klientů má veřejnou IP adresu a vytvoří si skrz veřejnou síť tunel pro své spojení.
- Klient-LAN – pokud se zaměstnanec firmy chce připojit do firemní sítě, a je na cestách, pomůže mu právě tento způsob.



Obrázek č. 14 VPN - možnosti spojení

Abychom mohli využít VPN, musíme mít ve své síti VPN server. Z tohoto serveru se stává brána, která umožní klientům připojit se z Internetu do naší sítě. Funkcemi brány jsou autentizace, šifrování a komunikace. Pro integritu se využívají tři způsoby:

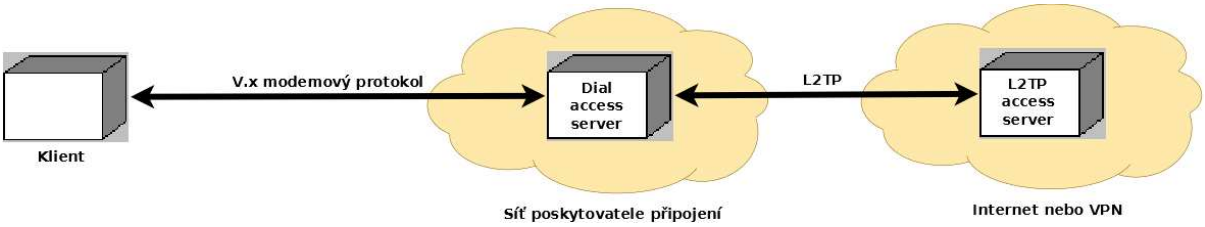
- Hashovací jednosměrná metoda – funkce generuje stejnou velikost, jakou mají šifrovaná data. Většinou se používají algoritmy DES, 3DES, AES atd. Při dešifrování jsou data ověřena algoritmem MD5 nebo SHA-1.
- Mac (Message authentication codes) – krátký údaj, který slouží k ověření zprávy. Vypočítá se soubor na základě sdíleného klíče, a poté je připojen k posílaným datům. Příjemce spočítá taky Mac a následně ho porovná s přijatým souborem.
- Ověření pomocí digitálního podpisu.

Šifrovací metodou, která zabezpečuje pakety TCP a UDP, je hojně využívaný IPSec. Tento protokol podporuje IP verze 4 a 6. Ve verzi 6 je tento protokol součástí doporučení. IPSec přidává do paketu sadu hlaviček pro jeho zabezpečení. Výhodou tohoto způsobu je, že je součástí infrastruktury. Proto je tolik podporován výrobci a málokdy se stane, že by různá zařízení (např. routery) nešla propojit mezi sebou.

Další typ VPN je GRE (Generic Routing Encapsulation). Slouží pro tzv. tunelování mezi dvěma body. Když paket vstupuje do „tunelu“, je mu přidána hlavička GRE header s cílovou adresou směrovače. Volitelně obsahuje autentizační pole či kontrolní součet. Na konci tunelu je tato hlavička odstraněna a ke svému cíli dál pokračuje jako normální paket.

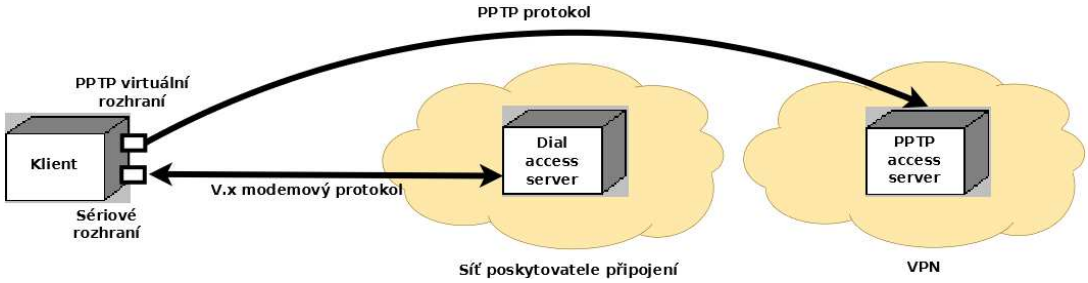
V dnešní době ve virtuálních sítích se hojně využívá způsobu komutovaného přístupu. Toto je zase metoda typu klient-server. V podstatě zde existují dva standardy :

L2TP – je typem povinného tunelování, neboli je inicializováno serverem, proto je pro klienta povinné. Pro vytvoření tunelu se spojí klient s dial-up nebo network access serverem. Pošle mu své autentizační údaje, které má u sebe uloženy nebo je získá z policy serveru. Tím se vytvoří dynamicky tunel L2TP.



Obrázek č. 15 L2TP tunel

Další variantou je PPTP. Je implementací „dobrovolného“ tunelování. Čili klient zde vytváří konfiguraci spojení. Je postaven nad protokolem PPP a při spojení s ISP se vytváří druhé neviditelné připojení k serveru PPTP. Tento protokol je vytvořen společností Microsoft.



Obrázek č. 16 PPTP tunel

Poslední variantou virtuálních sítí, která zde bude popsána, je VPN přes SSL. Je to typ klient-server. Pro tento způsob nám vystačí softwarové řešení. Je to celkem pohodlné, protože ke sdílení dat můžeme použít webové rozhraní. Před autentizací je nutné pouze potvrdit certifikát. Celá komunikace je po autentizaci šifrována. Tento typ VPN připojení využívá TCP port 443, stejně jako HTTPS protokol.

SSL (Secure Socket Layer) je vyzrálý protokol resp.vrstva vložená mezi vrstvu transportní a aplikační, která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran. Je dobře známý a populární ve světě zabezpečeného elektronického obchodování. Ustavení SSL spojení funguje na principu asymetrické šifry, kdy každá z komunikujících stran má dvojici šifrovacích klíčů:

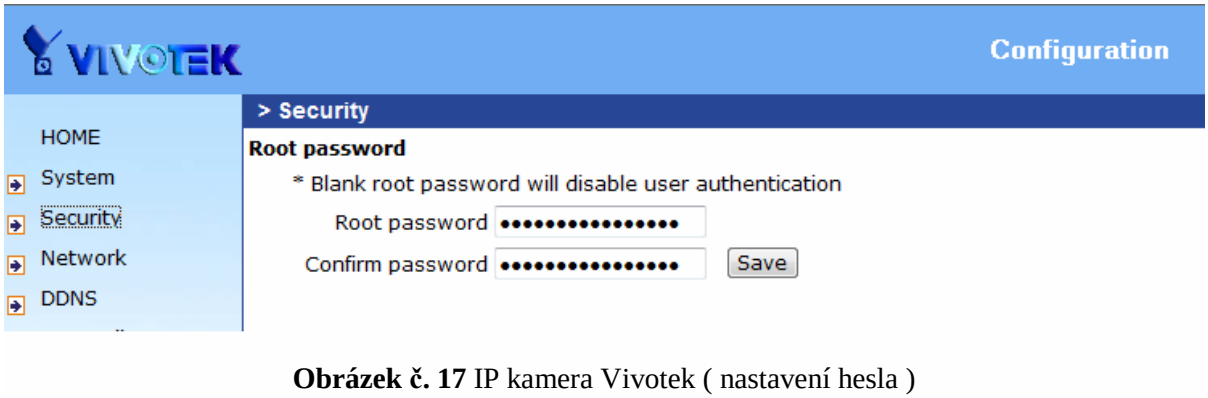
- Veřejný klíč
- Soukromý

Veřejný klíč je možné zveřejnit a pokud tímto klíčem kdokoliv zašifruje nějakou zprávu, je zajištěno, že ji bude moci rozšifrovat jen majitel použitého veřejného klíče svým soukromým klíčem.

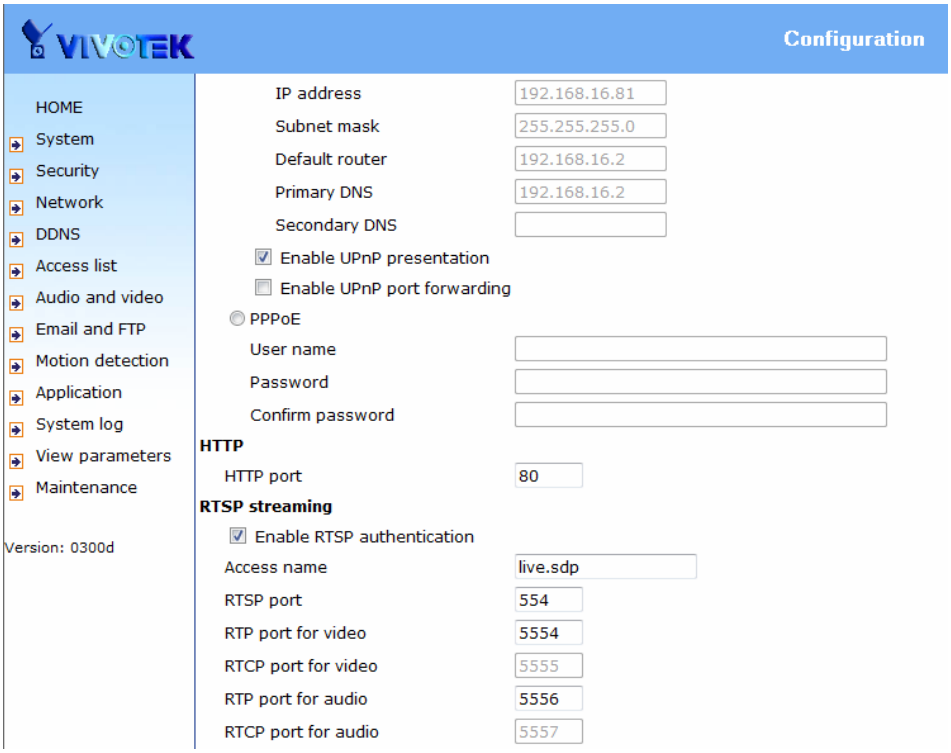
4.5 Příklad přenosu IP kamer

Téměř každá IP kamera dnes umožňuje zabezpečení pomocí autentizace, a access listu, dále nastavení portů a u IP kamer využívajících Wi-Fi - Advanced Encryption Standard (AES), což je schválený standard, který byl udělen symetrické blokové šifře Rijndael. Tato šifra využívá symetrického klíče, to znamená, že stejný klíč je použit pro šifrování i dešifrování. Délka klíče může být 128, 192 nebo 256 bitů. Metoda šifruje data postupně v blocích s pevnou délkou 128 bitů a vyznačuje se vysokou rychlostí šifrování. V současné době není veřejně znám žádný případ plného prolomení této metody ochrany dat.

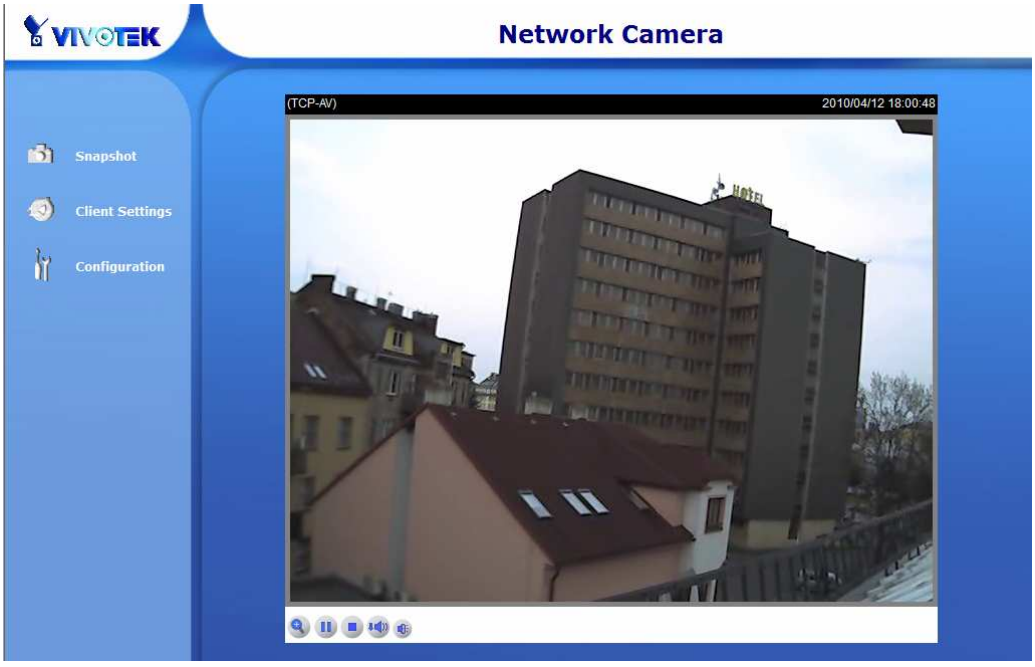
Jako příklad zde uvádím nastavení web kamery od výrobce VIVOTEK na obrázcích 17 – 19 včetně live obrazu.



Obrázek č. 17 IP kamera Vivotek (nastavení hesla)



Obrázek č. 18 IP kamera Vivotek (nastavení sítě)



Obrázek č. 19 IP kamera Vivotek (náhled live obrazu)¨

5. Doporučení a optimalizace nastavení zabezpečení přenosu dat dle velikosti a typu subjektu

Ve světě všudypřítomného Internetu je složité rozhodnout, jaká úroveň zabezpečení dat z kamerového systému je přiměřená, a pro konkrétní aplikaci dostačující. Všeobecně se dá doporučit, že web server kamerového systému by měl být hardwarově oddělen od ostatních systémů a dat používaných v domácnosti nebo firmě, což se v praxi moc nedodržuje a mnoho aplikací se tak vystavuje přímému útoku ze strany Internetu a riziku ztráty nebo poškození dat. Dále je nutné zvážit nebezpečí úniku těchto informací – dle charakteru snímaných prostor. Jinou prioritu ochrany budou mít data z kamerového systému v veřejných prostor, výrobních procesů, finančních ústavů nebo soukromých subjektů. V celkových nákladech na vybudování přiměřeně kvalitního kamerového systému je cena na zvýšení zabezpečení přenosu dat z těchto systémů zanedbatelná a téměř nulová.

- **Freeware software** – VPN, popřípadě GNU GPL **(**všeobecná veřejná licence GNU) svobodný software OPEN VPN

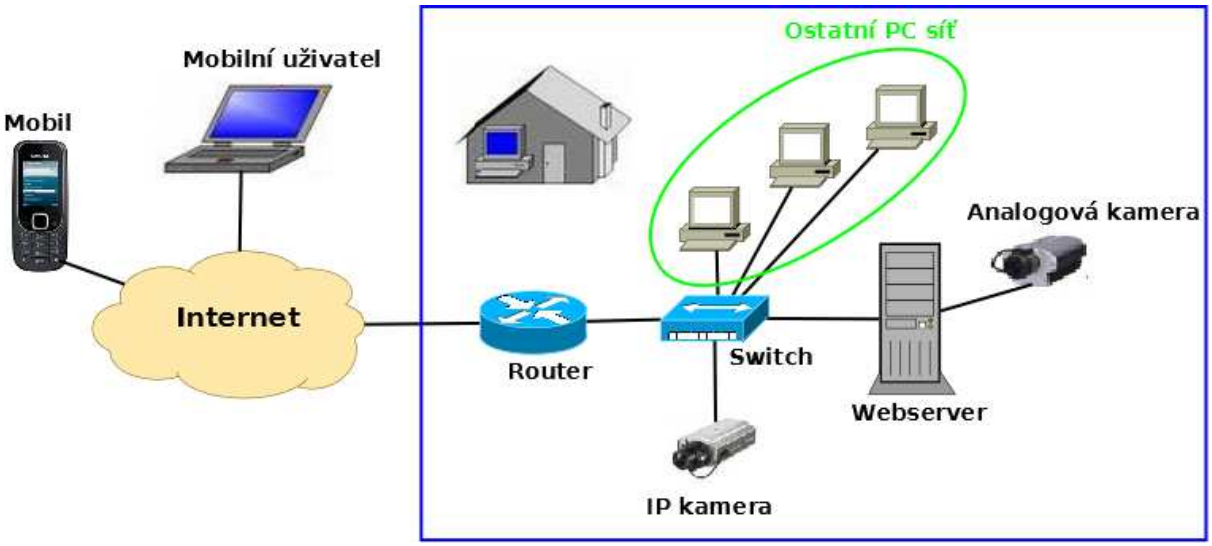
- **Placený software** – Radmin – jedna standardní licence Radmin stojí USD 49,- (aplikace Radmin Viewer je zdarma)

Ve všech dále uváděných úrovních zabezpečení přenosu dat z kamerového systému budu vycházet ze zkušenosti své praxe, kde bych vždy doporučil kamerový systém hardwarově sestavený ze stolního počítače vybaveného kartou do PCI slotu na zpracování videa dle rozsahu monitorovaných prostor. Důvodem je to, že digitální rekordéry na našem trhu nenabízejí takovou flexibilitu systému na jejich možné další rozšíření. Tento počítač, v našem případě video a web server dohromady, bude sloužit pouze pro kamerový systém a žádná jiná data zde zpracovávána ani archivována nebudou. Dále je nutné si uvědomit náročnost přenosu live obrazu, proto bych doporučil minimální rychlost upload (odesílání dat do Internetu) na straně serveru minimálně 256 kbit/s, aby byla zaručena přiměřená plynulost záznamu a všechny potřebné zálohy a archivace vždy provádět v rámci místní sítě. Poslední a důležitou podmínkou pro správnou funkci systému je veřejná IP adresa, bez které by byl vzdálený přístup ze strany sítě Internet nemožný. Na základě těchto informací se pokusím navrhnou řešení pro tři různé subjekty dle úrovně zabezpečení přenosu dat.

Úrovně zabezpečení přenosu dat z kamerových systémů:

- **Nízká úroveň** – zabezpečení pouze autentizací bez šifrování, vzdálený přístup přes webový prohlížeč, povolený RTSP stream pro mobil

Tato úroveň zabezpečení je vhodná pro monitoring obytných domů a malých provozoven, kde majitel chce mít jednoduchý a rychlý přehled o monitorovaných prostorech. Přístup do systému je umožněn z jakéhokoliv počítače v místní síti a Internetu pomocí webového prohlížeče a oprávněné autentizace uživatele. Pro přístup z mobilního telefonu jsou zde data zcela nechráněna, a pokud uživatel zná IP adresu web serveru a posloupnost příkazů, nic mu nebrání ve sledování on-line záznamu.



Obrázek č. 20 Nízká úroveň zabezpečení přenosu dat

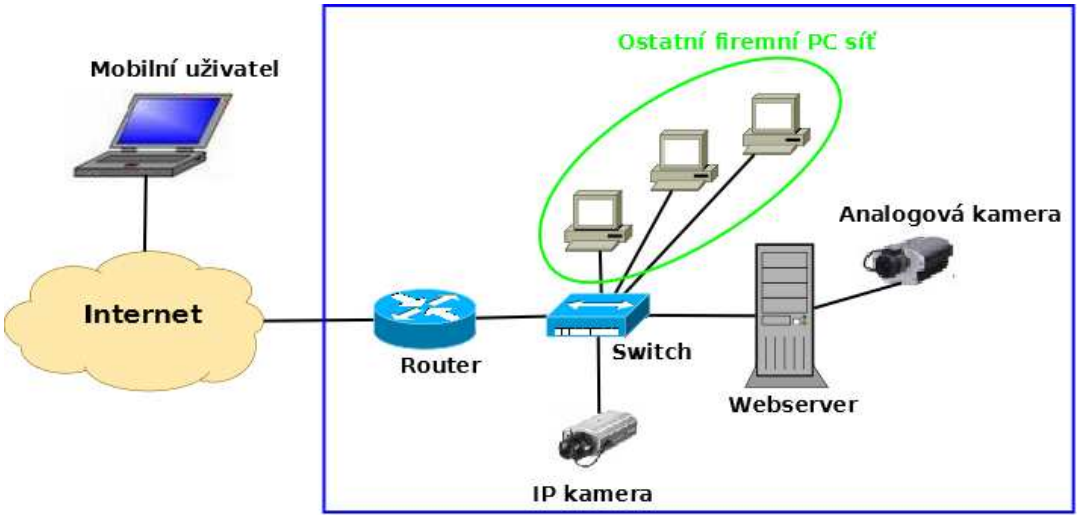
Pro správnou funkčnost systému znázorněného na obrázku č. 20 nám stačí na routeru v NAT tabulce povolit a nastavit směrování portů potřebných pro komunikaci kamerového web serveru. Přesná čísla portů jsou závislá na možnostech nastavení konkrétní video karty. V našem případě budeme muset povolit minimálně tři porty:

1. port pro web prohlížeč
2. port pro aplikaci na vzdálenou správu od výrobce systému
3. port pro RTSP stream

- **Střední úroveň** – použití softwaru pro vzdálenou správu, dodávaný výrobcem systému, doplněný firewallem, zakázaný RTSP stream pro mobil

Úroveň tohoto zabezpečení je vhodná pro monitoring středních firem, výrobních závodů a objektů s fyzickou ostrahou, kde kamerový systém je podporou právě pro tuto ostrahu a navíc slouží k monitorování výrobního procesu. Přístup do systému je umožněn pouze z oprávněného počítače v místní síti a Internetu, který je vybaven aplikací od výrobce pro vzdálenou správu daného kamerového systému. Jsou to rozsáhlejší instalace, kde je problematický přístup k samotnému video web serveru (většinou umístěným v dobře chráněné serverové místnosti), a je nutná vzdálená kontrola pořízených dat popřípadě sledování on-line provozu.

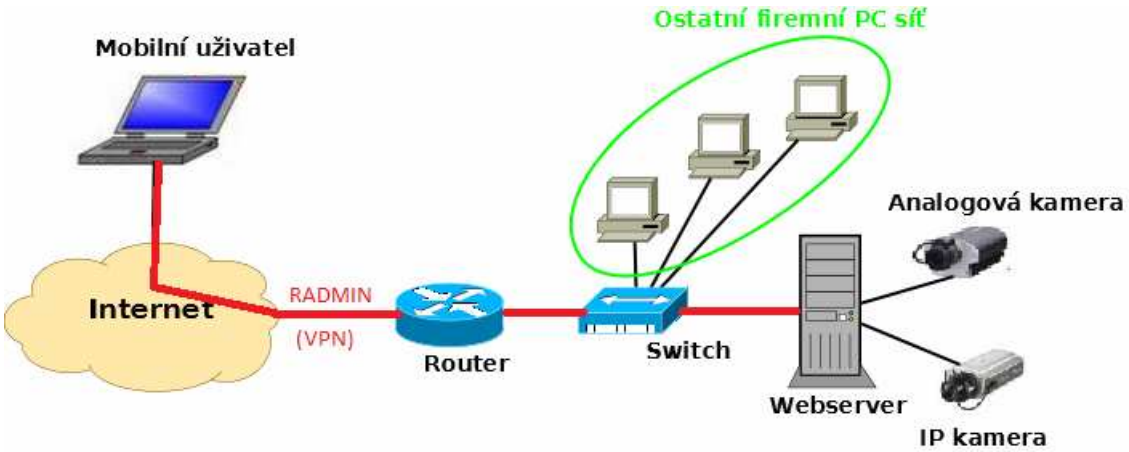
Pro nastavení systému podle schématu na obrázku č. 21 bude nutné na routeru v NAT tabulce opět povolit a nastavit směrování portů potřebných pro komunikaci kamerového web serveru. Většinou postačuje jediný port pro veškerou komunikaci, který lze libovolně měnit v závislosti na výrobci daného systému. Dále je nutné doplnit systém o hardwarový nebo softwarový firewall, který je nutno nastavit dle potřeb a požadavků klienta.



Obrázek č. 21 Střední úroveň zabezpečení přenosu dat

- **Vysoká úroveň** – použití pro vzdálenou správu dodávané výrobcem kamerového systému doplněné aplikací Radmin nebo VPN. Popřípadě použití aplikace VNC doplněné VPN, zakázaný RTPS stream pro mobil

Poslední mnou navrhovanou úroveň zabezpečení přenosu dat z kamerových systémů lze doporučit u aplikací s vysokou prioritou nebo rozsáhlou sítí poboček. U tohoto řešení (viz obr. č. 22) bych doporučil – pokud je to možné – hardwarové oddělení IP kamer od ostatní sítě a znemožnění přístupu neoprávněných uživatelů. Toho docílíme instalací další síťové karty do PCI slotu počítače, který nám slouží jako video a web server. IP kamery budou administrovatelné pouze ze stanice serveru.



Obrázek č. 22 Vysoká úroveň zabezpečení přenosu dat

Každé připojení k web serveru bude umožněno pouze se softwarem dodávaným výrobcem systému v zabezpečeném tunelu VPN nebo pomocí aplikace Radmin. S touto úrovní zabezpečení lze sice nesouhlasit a mít proti ní námitky, ale osobně si myslím, že je zcela dostačující pro běžné použití v praxi. Samozřejmě jsou realizovatelné i takové instalace, kde struktura a standardy firmy nedovolují žádné připojení ke kamerovým systémům ze strany sítě Internet, i když pro propojení svých dceřiných firem a poboček VPN tunely běžně používají.

6. Závěr

Stejně jako se vyvíjí jiné obory, tak i tento obor díky novým technickým možnostem, dostupnosti sítí a přenosu dat zaznamenal za posledních několik let značný posun dopředu. Troufám si říct, že tento obor je natolik dynamický, že při obhajobě své práce již budou na trhu další dokonalejší systémy zabezpečující jak přenos, tak i bezpečnost obrazu a dat.

Současné možnosti jak zabezpečit přenos obrazu a dat se odvíjí od jednoduchých až po kompletní a kvalitně zabezpečené přenosy. Technická dostupnost a nabídka na trhu všech systémů pro přenos obrazu a dat je v současné době velmi vysoká, což umožňuje v podstatě modelování systému „na míru“ s ohledem na požadavky a finanční kapacitu jednotlivých prostředků. Samozřejmě je i na výrobcích těchto systémů, aby dále vylepšovali zabezpečení vzdáleného přístupu, například využitím přenosového protokolu HTTPS, a tím zjednodušili obsluhu a bezpečný přístup pro uživatele bez nutnosti používat další software.

Často se setkávám s nejasnými požadavky na straně uživatelů těchto systémů, a tím také podhodnocené nebo ve velké míře nadhodnocené systémy, které nesplňuji rámcové využití přenosu dat a obrazu. Typickým příkladem jsou podnikatelské subjekty, které chtějí kompletní monitorování všech dostupných míst v místě svého podnikání, ale faktické využití tj. k čemu má tento monitoring sloužit, není zcela definováno. Vznikají zde často zbytečně naddimenzované systémy, které jsou finančně náročné na pořízení i provoz, ale jejich efektivita je v důsledku velmi nízká. Naopak jsou systémy, které neřeší základní požadavky zadavatele, neboť na jeho straně existují určitá omezení v technickém vybavení nebo zázemí pro přenos, a pak systém také nesplňuje očekávaný užitek.

Doporučuji vždy postavit vedle sebe cíl, který má přenos a bezpečnost dat zajistit, a efektivitu systému v propojení na to, kdo bude primárním uživatelem tj. kdo bude s on line nebo off line daty pracovat. Dále v jakém pojetí se budou reportovat zprávy z přístupů do systému pro sekundárního uživatele, a kdo bude zodpovídat za to, že bezpečnost přístupu k těmto získaným datům odpovídá jeho nastaveným požadavkům. Finanční stránka pořízení a provozu je také důležitým atributem pro rozhodování při výběru daného systému.

Jak jsem již zmínil v páté kapitole své práce, doporučuji provést vstupní screening požadavků na úroveň kvality přenosu a úroveň jeho zabezpečení z pohledu efektivity využití všech funkcí systému a pak připravit řešení „na míru“ a zkombinovat vždy nejvhodnější varianty z různých oblastí. Důležitým bodem pro návrh řešení je také obor podnikání podnikatelských subjektů, kdy v některých oborech jsou legislativně přesně určené limity, jak s pořízenými daty zacházet, např. bankovní sektor, policejní kontrola, státní a vládní sektor, ale i bezpečnostní agentury při ostraze objektů, které jsou povinné dodržovat zásady a úrovně bezpečnosti těchto přenosů.

Závěrem své bakalářské práce bych chtěl zmínit, že celkové pojetí bezpečnosti přenosu z kamerových systémů a doporučení, která jsem navrhl pro různé subjekty, je prakticky ověřeno v posledních šesti měsících na několika subjektech a má doporučení vycházejí jednak z mého dlouhodobého profesního působení v tomto oboru, ale také z intenzivního sebevzdělávání se s ohledem na dynamiku rozvoje tohoto oboru.

7. Použitá literatura a zdroje

[01] Bubeník, V.: Vzpomínka na počátky televize, CD katalog Amper 99 Terinvest a Proton, Praha 1999

[02] Frejlach, K.: Z historie radiotechniky, vydavatel Ing. Karel Frejlach, České Budějovice 1996

[03] OK2QX: 70 let od prvního dálkového přenosu, Praktická elektronika A Radio, 3 (1997)

[04] OK2QX: K počátkům televise, Praktická elektronika A Radio, 8 (1997)

[05] Glanc, A.: Amatérská televize, AR 6/71

[06] MacDonald, C: A: Compact Slow-Scan TV monitor, QST, March 1964

[07] dostupné na WWW
http://bruxy.regnet.cz/ok2mnm/cz_hist/oklgw/glanc_2.html [citace 2. 2. 2010]

[08] Čada, O.: Ohnivý drat
http://www.ocs.cz/text/AV_HA/IEEE1394.html [citace 14.2.2010]

[09] dostupné na WWW
http://maturita.spermik.info/soubory/.../VYSÍLACÍ%20ELEKTRONKY.doc [citace 28.2.2010]

[10] http://cs.wikipedia.org

[11] dostupné na WWW
http://www.nej-ceny.cz/clanky/nevite-si-rady-s-vyberem/nevite-si-rady-s-vyberem-kameroveho-systemu--popis-a-zaklady-ip-kamer-a-jejich-pripojeni/ [citace 13. 3. 2010]

[12] Hloušek, Z.: 2010 CCTV Kamerové systémy
http://www.zabezpeceni-domu.cz/index.php?nid=3643&lid=CZ&oid=1640154 [citace 18. 3. 2010]

[13] Redakce 2006
http://connect.zive.cz/node/194[citace 18.3.2010]

[14] Luhový, K.: 2003 VPN
http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=219&clanekID=225[citace 24.3.2010]

[15] Průcha, O.: 2005 VPN
http://home.zcu.cz/~ondrous/index.php?vyber=0[citace 24.3.2010]

[16] dostupné na WWW
http://www.radmin.cz/[citace 28.3.2010]

[17] dostupné na WWW
http://www.radmin.cz/products/radmin/security.php[citace 28.3.2010]

Přílohy:

Obsah přiloženého CD

Bakalářská práce SIM477.pdf