Sehr geerhte Professoren, liebe Mit-Studenten, ich begrüsse sie zur präsentation meiner Diplomarbeit mit dem Titel 'highly availabe KNX networks'

zum aufbau der präsentation: ich werde zuerst kurz auf das thema gebäudeautomation und auf den KNX standard selbst eingehen.
Danach werde ich erläutern welche defizite die ursprüngliche KNX spezifikation besitzt, und auch die bekanntesten erweiterungen und deren ziele vorstellen. Darauffolgend werde ich zusammenfassen warum diese erweiterungen nur bedingt ausreichen – dies ist quasi die motivitation für meine diplomarbeit, und welche ziele diese arbeit verfolgt.
abschliessend werde ich erklären wie genau mein proposal versucht diese ziele umzusetzen.

Gebäudeautomation beschäftigt sich im ursprünglichen sinn mit der steuereung und regelung von sogenannten HVAC-applikationen: HVAC steht dabei für 'heating, ventilation und air-conditioning'. Das hauptziel ist eine effiziente und zentrale verwaltung von raumparametern, und daraus folgend niedrigere verwaltungs- und energiekosten. ebenfalls nicht zu vergessen ist dass der raumkomfort in z.b. grossraumbüros sich direkt auf die produktivität der mitarbeiter auswirkt.

Wenn nun ein büro- oder fabriksgebäude mit der infrastruktur ausgestatttet ist um diese HVAC applikation steuern zu können liegt es sehr nahe diese für zusätzliche anwendungen einzusetzen – anwendungsfälle gibt es reichlich: diese reichen von raumbeleuchtungen und aufzugssystemen zu zutrittssystemen, alarmanlagen und sprinkler-und feuerschutzanlagen. Es ist allerdings schnell ersichtlich dass z.b. eine alarmanlage höhere anforderungen an die zuverlässlichkeit und integrität des zugrunde liegenden kommunikationssystems stellt als das schalten von beleuchtungselementen.. beim design von gebäudeautomationssystemene – im speziellen KNX – waren dies anforderungen welche ignoriert wurden. Dies hatte folgende gründe: erstens wurden die zu steuernden anwendungen als nicht-sicherheitskritisch eingestuft, zweitens erfolgte die kommunikation kabelgebunden, d.h. Pyhsikalischer zugriff auf das medium war notwendig. drittens fehlte oft ganz einfach die rechenleistung in den verwendeten embedded geräten zum umsetzen der notwendigen kryptografischen massnahmen. Die rechenleistung für nahtlose verschlüsselung steht allerdings heutzutage auch auf kleineren platformen zur verfügung. Weiters stellt sich heraus dass auch die beiden ersten argumente nicht auf realistischen annahmen beruhten. erstens ist es schlichtweg unmöglich bei einem automationssystem, welches über jahre wenn nicht jahrzehnte operabel sein soll, auch nur kurzfristigen zugriff auf das kabelmedium auszuschliessen. Die verwendung von kabellosen medien führt dieses argument grundsätzlich ad absurdum. Zweitens ist die annahme dass die ursprünglichen HVAC anwendungen nicht-sicherheitskritisch sind zu optimistisch – simple akte des vandalismus können durchaus spürbare ausfälle nach sich ziehen.

Folglich ist es notwendig, sicherheitsaspekte beim design von systeme zur heim- und gebäudeautomation zu berücksichtigen, bzw diese nachträglich entsprechend zu erweitern. Bei KNX exisitieren mehrere erweiterungen, welche etwas später kurz vorgestellt werden.

Ich möchte nun kurz definieren was hier unter 'sicherheitsaspekte' gemeint ist – im allgemeinen ist damit das erreichen von 'informationssicherheit' gemeint. Diese besteht aus drei säulen: confidentiality, integrity und availability, zusammengefasst zum CIA-triad. Confidentiality soll sensitive information vor unberechtigen entities schützen. Integrity stellt sicher dass schützenswerte daten nicht von dritten böswillig modifiziert werden können. Abschliessend stellt availability sicher dass ein system zuverässlich arbeitet und die definierten services den nutzern dieser services zur verfügung stehen.

---

damit komme ich zum zweiten teil meines vortrages, nämlich dem aufbau des KNX standards.

KNX enstand aus drei verschiedenen standards, nämlich EIB, dem 'europaean installation bus'; EHS, 'european home systems protokoll, und batibus, und wurde von der KNX association definiert. Es handelt sich um einen offenen standard, die vollständige spezifikation kann gegen eine gebühr bezogen werden, die verwendung danach ist frei. Zusätzlich ist eine zertifizierung möglich, allerdings nicht zwingend vorgeschrieben (KNX logo, ETS eintrag). Der standard orientiert sich am ISO OSI schichtenmodell, oberstes ziel ist grösstmögliche interoperabilität und damit hersteller-unabhängigkeit. Sensoren und aktoren werden mittels sogenannter 'group adresses' logisch zusammengefasst, womit die gewünschte semantik der kontrollapplikation erreicht wird.

Ganz oben im schichtenmodell stellt der applikation layer interfaces für die zugreifende applikation zur verfügung, z.b. das lesen oder schreiben von group values oder zur verteilung von netzwerkparamentern.

Der presentation layer, welcher eine system-unabhängige darstellung der ausgetauschten nachrichten garantiert, ist transparent. Um die angestrebte interoperabilität zu erreichen definiert KNX sogenannte 'data points': diese stellen die eigentlichen kontrollvariablen dar und werden zu 'data point types' mit einer definierten struktur zusammengefasst, wodurch eine einheitliche darstellung erreicht wird und der praesentation layer überflüssig wird.

Layer 5 oder 'session layer' ist ebenfalls transparent. Der Layer 4 oder transport layer stellt services für die end-zu-end verbindung zwischen quell- und zielhosts zur verfügung, wobei bei KNX unbestätigte als auch bestätigte übertragungsmodi möglich sind – für letzteren wird ein simpler handshake-mechanismus, ähnlich zu dem von TCP bekannten, verwendet.

Der wichtigste parameter des network layers ist die verwendete adresse. KNX verwendet 2 verschiedene arten von adressen: 'individual adresses' müssen eindeutig sein und adressieren ein bestimmtes gerät im netzwerk. 'group adresses' adressieren dagegen eine bestimmte gruppenvariable.

Layer 2 steuert den buszugriff und definiert verschiedene frameformate, wobei hier nur standard- und extended frames erwähnt seien.

Auf physikalischer ebene wurden verschiedene übertragungsarten definiert: erstens 'twisted pair' zur übertragung der steuerdaten über dezidierte kabelverbindungen. Powerline verwendet ein bereits vorhandenes stromnetz. Weiters besteht die möglichkeit der kabellosen kommunikation mittels 'radio frequency' sowie der austausch von daten mit IP hosts mittels KNX/IP, wobei letzteres hauptsächlich für backbone-traffic verwendet wird.

Wie bereits angemerkt definiert der ursprüngliche KNX standard keine ausreichenden sicherheitsmassnahmen. Dieses defizit wurde nachträglich durch die definition verschiedener extensions entschärft. Namentlich sind dies folgende:

- KNX data security arbeitet analog zu TLS und ermöglicht die end-zu-end-verschlüsselung zwischen KNX geräten, unabhängig vom verwendeten kommunikationsmedium
- EIBsec stellt ebenfalls verschlüsselte datenservices zur verfügung, allerdings mithilfe von dezidierten key-servern.
- KNX IP security fokussiert auf die verschlüsselung des backbone traffics und verwendet ebenfalls einen eigenen sicherheitslayer und ist damit ebenfalls mit TLS vergleichbar

Wenn also bereits erweiterungen exisitieren welche informationssicherheit garantieren – wozu dann eine zusätzliche? Der sinn dieser arbeitet ist die erhöhung der verfügbarkeit für kabelgebundene KNX netzwerke, wobei sowohl schutz gegenüber transienten hardwarefehlern gegeben sein soll, als

auch bei vorhandensein von böswilligen angreifern. Dies macht es notwendig das gesamte CIA triad zu berücksichtigen – die oben genannten erweiterungen fokussieren auf die komponenten confidentiality und integrity. Ein angreifer kann ein netzwerk dennoch durch kurzschliessen der kommunikationsleitungen lahmlegen. Auf die selbe fatale art und weise wirkt sich ein simpler, unvorhersehbarer kabelbruch aus.

Diese arbeit hat daher als ziel, alle 3 säulen des CIA triads in einem konzepte zu vereinigen. Dazu ist es notwendig, das kommunikationsnetzwerk gegen abhören und modifikation zu schützen, aber auch durch redundanz sicherzustellen dass zumindest ein kommunikationsweg verfügbar ist.