Security, privacy and trust in Internet of Things: The road ahead

Aluna: Joceleide Dalla Costa Mumbelli

Segurança Computacional

IoT

- Caracterizada por tecnologias heterogêneas
- Assim como as outras tecnologias de comunicação, também necessita de mecanismos de segurança para com os dados trafegados
- Apesar disso, devido a diferentes padrões e protocolos de comunicação envolvidos, não se pode aplicar os métodos de segurança tradicionais
- Além disso, o auto número de dispositivos conectados cria problemas de escalabilidade
- Esse trabalho apresenta os maiores desafios de pesquisa nessa área e suas soluções existentes no campo de internet das coisas.

Desafio de Segurança na IoT

- Autenticação e Confidencialidade
- Controle de acesso
- Privacidade
- Aplicação de Politica
- Confiança
- Segurança mobile
- Middleware Seguro

Autenticação e Confidencialidade

- Em um dos trabalhos citados no artigo, a autenticação usa um mecanismo de encapsulamento personalizado combinando comunicação criptografada entre plataformas, assinatura e autenticação
- Em outro trabalho, foi utilizado os padrões de internet inteligentes (protocolo DTLS). Baseado em RSA e 6LoWPANs
  - As avaliações demonstraram desse trabalho, mostraram integridade de mensagens, confidencialidade e autenticidade.
  - Aceitáveis nível de energia, latência e overhead.

Sobre Integridade e Confidencialidade

- Sistemas de gerenciamento de chaves (kms)
- Podem ser divididos em 4 categorias:
  - Key pool framework – Sofre de conectividade insuficiente
  - Mathematical framework – precisa que o servidor e o cliente estejam no mesmo local físico, o que não ocorre na IoT
  - Negotiation framework – Não se aplica a IoT pois nós clientes e servidores geralmente pertencem a redes diferentes, impedindo o funcionamento do framework
  - Public key framework – Tem muito overhead

Garantia de Confidencialidade

- Não existe uma solução única e bem definida para garantir a confidencialidade
- No campo de redes e sensores sem fio já foram realizadas muitas pesquisas e os seguintes questões foram levantados:
  - As propostas são adaptáveis considerando a heterogeneidade dos dispositivos.
  - Como e em qual camada cuidar da autenticação?
  - É possível que se use os mecanismos de segurança tradicional ou deve-se começar do zero?
  - Como lidar com chaves diferentes?
  - Qual mecanismo de distribuição de chaves é mais adequado?
  - Como garantir uma verificação de integridade ponto a ponto?

Alternativas de trabalhos recentes para g. confiabilidade (2015)

- Utilização do método de encriptação leve baseado em manipulação XOR
- lean key agreement protocol – Negocia uma chave de sessão com o nó sensor, usuário e gateway
- Eliptic Curve Cryptography – Mecanismo de estabelecimento de sessão

Controle de Acesso

- Refere-se a permissão de uso dos recursos associadas a diferentes dispositivos em um rede de IoT
- São divididos em duas categorias:
  - Detentores de dados – Usuários e coisas devem ser capazes de enviar dados somente com dados em relação a um tópico especifico
  - Coletores de Dados – devem ser capazes de identificar ou autenticar usuários e coisas como detentores de dados legítimos de onde a informação é coletada
- Em Iot também temos que lidar com o processamento de transmissão dados ou não, como em sistemas tradicionais de banco de dados, que tem dados discretos
  - Problemas de performace
  - Problemas de restrições temporais

Os maiores desafios relacionados ao Controle de Acesso

- Como garantir as permissões de acesso em um ambiente onde além de usuários, coisas também podem interagir com o sistema
- É mais efetivo explorar uma abordagem centralizada, distribuída ou semi distribuída de forma a gerenciar a escalabilidade?
- Como lidar com a grande quantidade de dados transmitidos em uma representação comum reconhecida?
- Como suportar a identificação de entidades?

Novas soluções propostas

- Novas soluções foram propostas de forma a responder algumas dessas questões, como o método de “subscriber” e um esquema de grupo de membro para lidar com o controle de acesso.
  - Exemplo PUF e eSIM
- Outro trabalho faz comunicação multicast segura adotando uma chave de segurança comum, denotada chave de grupo, compartilhada por muitos pontos de comunicação. Esssas chaves são gerenciadas e distribuídas com uma abordagem centralizada

Privacidade em IoT

- Exemplos de aplicações de IoT: monitoramento demoto de pacientes, controle de consumo de energia, controle de trafego, sistema de estacionamento inteligente, cadeia de produção, proteção civil,etc.
- É necessária a proteção dos dados pessoais do usuário relacionados a seu movimento, habito e interações com outro pessoas

- Em um dos trabalhos é utilizado sistema de tagging para gerenciamento de privacidade.

Privacidade em IoT

- Em outro trabalho(domínio estático atribuído a um nó) é proposto um DNS melhorado com proteção de privacidade para dispositivos inteligentes, o qual pode autenticar identidades de usuário originais e recusar acesso ilegal aos dispositivos.
- Outro autor apresenta um protocolo totalmente decentralizado e anônimo para autenticação de aplicações IoT. Utiliza a abordagem baseada em sistema de credenciais “multi-show”, evitando que as chaves geradoras sejam descobertas.
- Em outro trabalho é utilizado um protocolo de autenticação mútua de troca de chaves para sistemas WSN e RFID. Esse protocolo integra um gerador de números randômicos na tag e adota funções hash de uma-mão, a atualização de chaves em tempo real e um mecanismo de backup de chaves para reduzir riscos de replay, replicação, negação de serviços, etc.

Em resumo

- Privacidade em IoT ainda está apenas parcialmente satisfeita.
- Ainda existe grandes problemas de pesquisa a serem investigados relacionados a necessidade de definir politicas de privacidade começando de um modelo bem definido
- Além disso, lidar com a escalabilidade e o ambiente dinâmico de cenários de IoT.

Confiança em IoT

- Os requisitos de confiança estão estritamente relacionar ao gerenciamento de identidade e aos problemas de controle de acesso.
- Como a maioria dos objetos inteligentes são relacionados a humanos, geralmente eles ficam expostos em áreas publicas e comunicam-se por tecnologias sem fio, tornando-se vulneráveis a ataques
- Objetos inteligentes precisam cooperar entre si
- As relações sociais consideradas são: amizade, comunidade e propriedade
- Nós maliciosos visam quebrar a funcionalidade básica de IoT com ataques relacionado a confiança como

Protocolo de gerenciamento de confiança

- Em um dos trabalhos é proposto um protocolo distribuído onde:
  - Dois nós que entram em contato entre si podem avaliar um ao outro e trocar avaliações de confiança a respeito de outros nós
  - Os parâmetros de avaliação são: honestidade, cooperatividade e interesse da comunidade.

- Em outro trabalho é utilizado o conceito de Social Internet of Thing(SIoT), que tem por base a integração de conceitos de redes sociais em IoT.
  - Cada nó calcula a confiança de seus amigos com base em sua própria experiência e na opinião de amigos em comum.
  - Quando dois dispositivos confiam um ao outro, ele trocam serviços e recursos

Visão geral sobre Confiança em IoT

- As soluções existentes atualmente exploram diferentes técnicas para garantir a confiança no cenário IoT
- Isso inclui modelos hierárquicos, mecanismos de reputação, abordagens derivadas de redes sociais, técnicas fuzzy mecanismos baseados no comportamento passado dos nós ou em estratégias de roteamento.
- Apesar disso a definição de uma abordagem totalmente distribuída e dinâmica que se encaixa na escalabilidade e flexibilidade do contexto IoT ainda não existe

Alguns problemas ainda existentes

- Introdução de uma linguagem de negociação de confiança bem definida
- Definição de um sistema de gerenciamento de identidade de objetos
- Desenvolvimento de um mecanismo de negociação de confiança de forma a controlar o acesso ao fluxo de dados.

Execução em IoT

- Aplicação de políticas refere-se aos mecanismos utilizados para forçar a aplicação a um conjunto de ações definidas em um sistema
- Politicas são regras de operação que devem ser aplicadas de forma a manter a ordem, segurança e consistência dos dados
- No cenário de IoT, não existem soluções viáveis ou analises detalhadas nesse sentido.

Exemplo de problema na garantia de aplicação de politicas

- Em um sistema de saúde, a cooperação e comunicação entre farmácia, hospital e escola medica é essencial.
- Cada um deles tem seus próprios mecanismos de aplicação de politicas, para proteger seus dados proprietários e registros de pacientes
- O problema na comunicação entre esses domínios é que uma aplicação de politica "entre-domínios" se torna um componente essencial,
- Na pratica, esses domínios utilizam diferentes politicas especificas para sua plataforma
- Quando uma comunicação é necessária, os departamentos técnicos dos domínios envolvidos devem trabalhar junto para avaliar se é possível ou não a interoperabilidade de seus sistemas
- O mesmo acontece com problemas de privacidade em redes sociais

Aplicação de políticas em IoT

- Não existe nenhuma solução especifica para IoT que forneça garantia de aplicação de politicas de segurança e privacidade.
- Alguns estudos tem sido realizados para definir uma linguagem para especificações de politicas de privacidade, mas uma padronização que tenha aplicação especifica ao paradigma de IoT ainda não existe.

Middlewares seguros em IoT

- Devido ao grande numero de dispositivos heterogêneos no cenário de IoT, diversos tipos de middleware são aplicados de forma a garantir a integração e a segurança de dispositivos e dados na mesma rede.
- Com o uso de middleware, as trocas de informações devem respeitar restrições de proteção especificas.

Exemplos de Middlewares existentes

- VIRTUS – middleware de IoT baseado no XMPP promove segurança em comunicações baseadas em eventos com cenário IoT
  - Além da segurança oferecida pelo XMPP, o middleware oferece canal de comunicação confiável e seguro para aplicações distribuídas, protegidas com autenticações (TLS) e encriptação(SASL)
- Otsopack- possui duas funcionalidades principais:
  - Foi desenvolvido para ser simples, modular e extensível
  - Roda em diferentes plataformas computacionais, incluindo Java SE e Android

Funcionamento: Cada aplicação escreve informações semanticamente anotadas em um espaço compartilhado, e outros aplicativos ou nós podem consulta-lo

Principais questões a respeito de middlewares

- Como dispositivos heterogêneos e usuários podem interagir dinamicamente e entrar em acordo com o mesmo protocolo de comunicação, garantindo também segurança e privacidade?
- Como fazer uma solução viável para diferentes plataformas e portanto não depender de interfaces ou protocolos ?

Segurança mobile em IoT

- Nós moveis em IoT geralmente migram de um cluster a outro, no qual protocolos de criptografia são necessário para garantir rápida identificação, autenticação e proteção de privacidade.

- Em um dos trabalhos é apresentado um protocolo ad hoc.
  - Esse protocolo contem uma "mensagem de requisição valida" e uma "mensagem de resposta de autenticação", que rapidamente implementa identificação, autenticação e proteção de privacidade.
  - Apresenta menos overhead de comunicação, mais segurança e mais propriedades de proteção de privacidade

Exemplos de protocolos para mobilidade em IoT

- Outro autor utiliza sistemas de RFID, baseados em EPC(Electronic Produc Code) para automaticamente identificar objetos marcados, utilizando sinais de radiofrequência, sem contato direto.

- Em outro trabalho um esquema de handshake seguro entre nós móveis é posposto em um sistema de transporte inteligente.
  - Um nó móvel verifica, por meio de um canal de comunicação inseguro, a legitimidade de um nó sensor comum por meio de uma negociação de handshake privada.
  - Dessa forma uma hierarquia móvel é estabelecida de forma a consultar uma WSN de forma segura.

Projetos em andamento

Table 3
Contribution of ongoing European projects on IoT security.

	Butler	EBBITS	Hydra	uTRUSTit	iCore	HACMS	NSF	FIRE	EUJapan
Authentication	x			x	x	x	x	x	
Confidentiality	x	x	x		x	x	x	x	x
Access Control	x	x		x	x	x	x	x	
Privacy	x				x		x	x	x
Trust				x	x		x		
Enforcement									
Middleware		x	x		x				
Mobile	x						x		

Conclusão

- O avanço do cenário IoT necessita do desenvolvimento de serviços customizados de segurança e privacidade.
- Esse artigo apresentou um aparato geral de tecnologias desenvolvidas ou em desenvolvimento na área de segurança em IoT, além de levantar questões que ainda precisam ser respondidas.
- Soluções aplicáveis que sejam capazes de garantir: confidencialidade, controle de acesso e privacidade para usuários e coisas, confiabilidade entre dispositivos e usuários e conformidades com as políticas de privacidade.

Security, privacy and trust in Internet of Things: The road ahead

Aluna: Joceleide Dalla Costa Mumbelli

Segurança Computacional