# Autenticação de Sensores usando Eventos Físicos

Alunos: Gabriel Zeferino, Gustavo Cousseou, Thobias Stahlschmidt

# Introdução

- Tecnologias pervasivas
- Aplicações Smart
- Sensores (Complexos industriais, edificações, veículos, eletro utilitários e dispositivos biomédicos)
- Segurança: autenticação de sensores (ICP, HMAC, PUF e one-time)
- Soluções custosas

# Introdução

- Deseja-se autenticação sem recurso adicional
- Sensores monitoram o mesmo evento físico
- Atacante não possui acesso ao ambiente físico (eavesdrop)
- Eventos físicos evidenciam simultaneidade e co-alocação.
- Ataques relay e replay
- Autenticação baseada em eventos físicos

# Trabalhos Relacionados

- Biometria Comportamental
- Acelerômetro: Jeito de andar, chacoalhados, aperto de mão
- Redes, canal de rádio

# Propriedades de um Evento Físico

- Tecnologia pervasiva - camada física, controle
- Imprevisível e único
- Quando entidades descrevem o mesmo evento físico
- Co-alocação: mesma localização (relay)
- Simultaneidade: capturam o evento ao mesmo tempo (replay)

# Modelo de Ataque

- Duas entidades A e B trocam informações
- Entidade maliciosa M sem acesso ao ambiente físico
- Propõe-se A e B fortalecer a autenticação através de evento físico que M desconhece.

# Autenticação baseada em Eventos Físicos

- Identificador mensurado por A e B, M difícil de reproduzir
- M não tem acesso, identificador obtido por canal exclusivo, protege contra eavesdropping
- Satisfazem condição de co-alocação e simultaneidade
- Pode-se implementar em sistemas com funcionalidades de sensoriamento sem hardware adicional.

# Mecanismo de autenticação

- Conjunto de N sensores, dado por grandezas físicas
- Um conjunto P extrai as características de um sinal para compor o identificador
- Embora obtidos de um mesmo evento, não pode-se esperar que sejam idênticos
- Função de comparação e limiar
- C(IDa,IDb) <= Th

# Estudo de caso: Teste de impacto

- Teste de impacto veicular
- Sensores(acelerômetro e células de carga) posicionados em diferentes pontos do veículo e no ATD(Antropomorphic Test Dummy)
- DAS(Data Acquisition System)
- DAS envia os dados para um centro de análise
- Dados armazenados em um banco de dados

# O Modelo de Ataque

- Resultados de teste afetam as decisões de consumos
- Pode-se alterar o resultado de teste
- Interceptar e modificar o sinal antes de ser recebido pelo Control (relay)
- Substituir o sinal de um sensor legítimo por outro legítimo obtido em teste prévio (replay)

# Autenticação Baseada em Eventos Físicos

- Propõe-se implementar autenticação para os sensores dentro do ATD durante o teste de impacto
- Cada colisão produz um resultado único
- Control é responsável por autenticar um sensor
- Identificador de evento físico
- Função de comparação
- Satisfazer o critério de limiar estabelecido

# Cenários de Autenticação

- ATD → acelerômetros e/ou células de carga
- Sensores vizinhos (cabeça e pescoço) NS
- Sensores redundantes RS

# A Colisão como Evento Físico

- Obtém-se o vetor de aceleração/força Rs
- bEvent → 50ms tensão do cinto
- eEvent →  pico da desaceleração

# Identificador

- O identificador do evento deve ser obtido extraindo características relevantes em cada sensor
- Utiliza-se duas técnicas de fusão de dados
- Filtro de Médias Móveis (MAF) com passo variável (elimina operações com float, menor esforço)
- Função de extração de informação, projetada  a partir de testes empíricos

# Experimentos Práticos

- Autenticação avaliada por meio de experimento prático usando dados de teste de impacto da NHTSA(National Highway Traffic Safety Administration).
- Coletados 100 casos de testes com o protocolo de colisão frontal

# Cenário NS

- Atacante tenta corromper um dos sensores a fim de comprometer o resultado do teste
- Existem 4 casos possíveis:

# Tipos de Ataques

- HxH: Compromete sensor da cabeça utilizando um sinal legítimo de um sensor de cabeça
- NxN: Compromete sensor do pescoço utilizando um sinal legítimo de um sensor de pescoço
- HxN: Compromete sensor da cabeça utilizando um sinal legítimo de um sensor de pescoço
- NxH: Compromete sensor do pescoço utilizando um sinal legítimo de um sensor de cabeça

# Eficiência

- Avaliada usando métricas comuns em sistemas biométricos.
- FRR (False Rejection Rate)
- FAR (False Acceptance Rate)
- Para problema de autenticação espera-se um menor valor de FAR do que um baixo de FRR

# Eficiência

- Se uma autenticação legítima é negada, a autenticidade pode ser verificada por um segundo método
- Se uma tentativa de ataque é aceita pelo processo de autenticação, tem-se uma falha de segurança
- FRR em 18%
- FAR abaixo de 1% menos para HxN (1,1%)

# Eficiência

- Conclui-se que para este caso, as funções de geração de identificador devem ser melhoradas
- Redução do FRR

# Cenário RS

- Sensores redundantes da cabeça
- Dois sensores no mesmo local apresentam alta correlação
- Repete-se o mesmo experimento do cenário NS

# Eficiência

- As métricas FRR e FAR foram reduzidas
- FRR em 0%
- FAR em 0.08%
- Mostra que sensores redundantes possuem elevada eficiência na autenticação baseada em eventos físicos

# Autenticação de Sensores usando Eventos Físicos

Alunos: Gabriel Zeferino, Gustavo Cousseou, Thobias Stahlschmidt