III WSD

3ER WORKSHOP

SUBESTACIÓN DIGITAL
Y EQUIPOS PRIMARIOS
"CIBERSEGURIDAD PARA SAS"

Escenarios de Ataque Maqueta 1

CONPROVE

weg

SIEMENS

Belden

ORGANIZA cigre Paraguay

APOYA ITAIPU BINACIONAL

Cibersegurança nos Equipamentos CONPROVE

- Conexão via USB - > - Isolada
- Conexão via Rede -> - Criptografada
  - Senha
- Firmwares -> - Criptografados
  - Assinados Digitalmente
- Processador -> - TPM 2.0 (Trusted Plataform Module)
- Entre outros ...

CUIDADO / CUIDARSE

Ataque em andamento ...

Sc1 · Reconhecimento Passivo no Barramento de Estação (Sniffing)

Barramento de Estação | Nível de Automação: Estação / Baia | Impacto: Baixo

- **1. Identificação do Ataque**
  Tipo de Ataque: [RECONHECIMENTO] / [SNIFFING] — Passivo
  Nível de Automação: Estação / Bay Alcance / Nível de Impacto: Baixo / NA
- **2. Alcance e Objetivo**
  Nó / Ativo Alvo: Todos os nós conectados ao Barramento de Estação (SCADA, IHM, IEDs, GMC, etc.)
  Função Alvo (SPAC): NA
- **3. Vetor e Pré-condição do Ataque**
  Um atacante consegue acesso físico a uma porta trunk;
  Exploração de vulnerabilidades;
  Captura de tráfego completo.

- **4. Procedimento de Teste**
- **Equipamentos de Teste**: Conprove CE-MNET – Equipamento de injeção e monitoramento.
- **Descrição da Conexão**:
  O CE-MNET conecta-se fisicamente à rede do barramento de estação por meio de uma porta trunk do switch, permitindo a observação do tráfego do barramento sem necessidade de interação ativa com os dispositivos.
- **Configuração de Rede**:
  Porta do switch configurada como trunk para permitir a captura de todo o tráfego do segmento da estação.
- **Descrição da Execução**:
  O CE-MNET opera em modo passivo (sem injeção de tráfego). Captura e analisa todos os quadros que circulam no barramento de estação: protocolos MMS, ARP, STP e tráfego de administração. A execução ocorre por meio da visualização em tempo real dos nós ativos (MACs, IPs, protocolos) para coleta de parâmetros detalhados. As informações obtidas serão utilizadas como insumo para cenários posteriores.

- **Objetivo:**
  - Identificar os dispositivos presentes na rede
  - Obter informações dos nós ativos (endereços MAC, IP, etc.)
  - Caracterizar os fluxos de comunicação
  - Obter informação suficiente para suportar cenários de ataque ativo posteriores
- **5. Resultados Esperados**

  Sem Mitigação: Comprometimento da confidencialidade — o atacante obtém um mapa completo da topologia, dispositivos e comunicações do barramento de estação sem ser detectado.

Sc2 · Reconhecimento Passivo no Barramento de Processo (Sniffing)

Barramento de Processo | Nível de Automação: Processo | Impacto: Baixo

- **1. Identificação do Ataque**
  Tipo de Ataque: [RECONHECIMENTO] / [SNIFFING] — Passivo
  Nível de Automação: Processo Alcance / Nível de Impacto: Baixo / NA
- **2. Alcance e Objetivo**
  Nó / Ativo Alvo: Todos os nós conectados ao Barramento de Processo (IEDs de bay, Merging Units, switches de processo)
  Função Alvo (SPAC): NA
- **3. Vetor e Pré-condição do Ataque**

  Um atacante consegue acesso físico a uma porta trunk;

  Exploração de vulnerabilidades;

  Captura de tráfego completo.

- **4. Procedimento de Teste**
  Equipamentos de Teste: Conprove CE-MNET
- **Descrição da Conexão**:
  O CE-MNET conecta-se fisicamente à rede do barramento de estação por meio de uma porta do switch.
- **Configuração de Rede**:
  Porta do switch de processo configurada em modo trunk para captura de todo o tráfego do segmento de processo.
- **Descrição da Execução**:
  O CE-MNET opera em modo passivo. Captura e analisa quadros GOOSE, Sampled Values (SV/SMV) e mensagens PTP que circulam no barramento de processo. A execução ocorre por meio da visualização em tempo real dos nós ativos para coleta de parâmetros detalhados.

- Objetivo:
  - Identificar os dispositivos presentes na rede
  - Obter informações dos nós ativos (detalhes de mensagens GOOSE, SV, PTP)
  - Caracterizar os fluxos de comunicação
  - Obter informação suficiente para suportar cenários de ataque ativo posteriores
- **5. Resultados Esperados**

  Sem Mitigação: Comprometimento da confidencialidade — o atacante obtém informações completas do barramento de processo, possibilitando ataques de injeção posteriores.
- **6. Medidas de Mitigação**

  A serem realizada pela Siemens

Sc3 · Injeção de Frames GOOSE Fabricadas/Reinjetadas

Barramento de Processo | Nível de Automação: Processo | Impacto: Alto

- **1. Identificação do Ataque**
  Tipo de Ataque: [INJEÇÃO] / [FABRICAÇÃO] / [REPLAY]
  Nível de Automação: Processo Alcance / Nível de Impacto: Alto — Proteção (P)
- **2. Alcance e Objetivo**
  Nó / Ativo Alvo: IEDs de bay e Merging Units (MUs) conectados ao Barramento de Processo
  Função Alvo (SPAC): Proteção (P)
- **3. Vetor e Pré-condição do Ataque**

  Um atacante com conhecimento prévio da rede e de suas configurações consegue acesso físico a uma porta trunk do switch de processo. Explora configurações inseguras de controle de acesso, ausência de mecanismos de autenticação, falta de monitoramento de dispositivos não autorizados e segmentação inadequada da rede.

  Atacante é capaz de injetar frames GOOSE.

- **4. Procedimento de Teste**
  Equipamentos de Teste: Conprove CE-MNET (funções de injeção GOOSE), Conprove CE-7012 (caixa de ensaios para verificação de efeitos em IED/MU)
- Descrição da Conexão:
  O equipamento CE-MNET conecta-se fisicamente à rede do barramento de processo por meio de uma porta do switch, a partir da qual realiza a injeção de frames GOOSE.
  O equipamento CE-7012 conecta-se ao IED de bay com o objetivo de observar e verificar os efeitos produzidos pela injeção no comportamento do sistema.
- Configuração de Rede:
  Porta trunk no switch de processo com acesso às VLANs de processo. O CE-MNET deve ter visibilidade dos IEDs e MUs alvo.
- Descrição da Execução:
  São executados dois subcenários de injeção GOOSE.

- **Objetivo:**
  - Emissão de comandos de operação não autorizados (por exemplo, abertura/fechamento de disjuntores)
  - Burlar a leitura de estado do Disuntor
  - Execução de ordens falsas para IEDs, afetando a lógica de controle
- **Subcenários de Execução**
  - **Sc3-A — Injeção GOOSE no IED — Burlar Leitura de Estado do CB (Supervisão Falsa)**
    O CE-MNET fabrica frames GOOSE simulando ser a MU, com valores de estado do CB invertidos (aberto → fechado ou vice-versa).
  - **Sc3-B — Injeção GOOSE na MU — Acionar o CB de Forma Indevida (Comando de Trip)**
    O CE-MNET fabrica frames GOOSE simulando ser o IED, com um comando de trip/operação direcionado à MU.

- **5. Resultados Esperados**

  Sem Mitigação: Comprometimento da integridade — perda de integridade da supervisão devido a mensagens GOOSE injetadas que reportam estados falsos do CB; perda de integridade de proteção/controle por comandos GOOSE de trip/operação injetados de forma inadequada.

- **6. Métodos de Detecção e Monitoramento**

  Ferramentas: CONPROVE e WEG

- **7. Medidas de Mitigação**

  SIEMENS

Sc4 · Injeção de Frames SMV (Sampled Values) Fabricadas

Barramento de Processo | Nível de Automação: Processo | Impacto: Alto

- **1. Identificação do Ataque**
  Tipo de Ataque: [INJECTION] / [Fabrication] / [Replay]
  Nível de Automação: Processo
  Alcance / Nível de Impacto: Alto — Proteção (P), Controle (C)
- **2. Alcance e Objetivo**
  Nó / Ativo Alvo: IEDs de bay conectados ao Barramento de Processo
  Função Alvo (SPAC): Proteção (P), Controle (C)
- **3. Vetor e Pré-condição do Ataque**
  Vetor de ataque: Um atacante com conhecimento prévio da rede e de suas configurações consegue acesso físico a uma porta trunk do switch de processo. Explora configurações inseguras de controle de acesso, ausência de mecanismos de autenticação, falta de monitoramento de dispositivos não autorizados e segmentação inadequada da rede (física e VLAN), sendo capaz de injetar frames SMV.

- **4. Procedimento de Teste**
  Equipamentos de Teste: Conprove CE-MNET (injeção SMV), Conprove CE-7012 (caixa de ensaios para verificação de efeitos)
- Descrição:
  O CE-MNET, conectado em uma porta trunk, captura frames SMV legítimos da MU e as reinjeta em direção ao IED, criando uma segunda stream SMV. Isso pode provocar rejeição de amostras (perda de supervisão e bloqueio da proteção 87L).

- Objetivo:
  - Atrapalhar a medição de corrente/tensão percebidos pelo IED (supervisão)
  - Bloquear operações de proteção

- **5. Resultados Esperados**
  Sem Mitigação: Comprometimento da integridade/disponibilidade — perda de integridade da supervisão, proteção e controle devido a mensagens SMV injetadas com medições falsas.

- **6. Métodos de Detecção e Monitoramento**
  Ferramentas: CONPROVE e WEG

- **7. Medidas de Mitigação**
  SIEMENS

Sc5 · Injeção de Frames PTP Fabricados

Barramento de Processo | Nível de Automação: Bay | Impacto: Alto

- **1. Identificação do Ataque**
  Tipo de Ataque: [INJEÇÃO] / [FABRICAÇÃO] — Sincronismo de Tempo
  Nível de Automação: Bay / Processo Alcance / Nível de Impacto: Alto — Supervisão (S), Proteção (P)
- **2. Alcance e Objetivo**
  Nó / Ativo Alvo: Todos os nós do Barramento de Processo com sincronismo de tempo (IEDs, MUs, switches com PTP)
  Função Alvo (SPAC): Supervisão (S), Proteção (P)
- **3. Vetor e Pré-condição do Ataque**
  Vetor de ataque: Um atacante consegue acesso físico a uma porta do switch de processo. Explora configurações inseguras de controle de acesso, ausência de mecanismos de autenticação, falta de monitoramento de dispositivos não autorizados e segmentação inadequada da rede.

- Nesse contexto, o atacante pode injetar pacotes PTP fabricados, se passando pela fonte legítima de sincronização de tempo. Por meio de uma porta configurada como trunk com acesso à VLAN de sincronismo da rede, consegue alterar a referência temporal dos dispositivos do sistema.
- Com essa técnica, o atacante modifica o tempo percebido pelos equipamentos, afetando a coerência temporal de eventos, registros e a correlação de informações dentro do sistema de automação.
- **4. Procedimento de Teste**
  Equipamentos de Teste: Conprove CE-MNET (injeção PTP)
- Descrição da Conexão:
  O CE-MNET conecta-se a uma porta trunk do switch de processo para injetar frames PTP fabricadas.

- Configuração de Rede:
  Porta do switch de processo com acesso às VLANs de sincronismo. O CE-MNET deve ter visibilidade dos nós PTP do segmento.

- Descrição da Execução:
  São executados dois subcenários de injeção de sincronismo.

Objetivo:

Gerar eventos no IED que bloqueiem a proteção 87L

- **4a. Subcenários de Execução**
- **Sc5-A — Injeção PTP**
  O CE-MNET gera e injeta frames PTP (Announce, Sync, Follow_Up, Delay_Req) fabricadas no barramento de processo com o objetivo de participar do processo BMCA (Best Master Clock Algorithm) como um Grand Master Clock (GMC) fictício. Neste subcenário busca-se substituir a fonte de sincronismo real pela fonte simulada pelo atacante.
- **Sc5-B — Injeção PTP com alteração de VLAN**
  O CE-MNET injeta frames PTP fabricadas, porém com VLAN que o isola o ataque apenas em um dos lados, ocasionando fontes de sincronismo diferentes entre os dois terminais da linha, e assim bloqueando a proteção 87L.

- **5. Resultados Esperados**
  Sem Mitigação:
  - a) proteção funcional
  - b) proteção 87L bloqueada
- **6. Métodos de Detecção e Monitoramento**
  Ferramentas: CONPROVE e WEG
- **7. Medidas de Mitigação**
  SIEMENS

Sc6 · Injeção de Frames Malformados no Barramento de Processo (DoS a IEDs/MUs)

Barramento de Processo | Nível de Automação: Processo | Impacto: Alto

- **1. Identificação do Ataque**

  Tipo de Ataque: [INJECTION] / [Fabrication] / [DoS]

  Nível de Automação: Processo

  Alcance / Nível de Impacto: Alto — Supervisão (S), Proteção (P), Controle (C)

- **2. Alcance e Objetivo**

  Nó / Ativo Alvo: Nós do Barramento de Processo: IEDs de baia, Merging Units (MUs), switches de processo

  Função Alvo (SPAC): Supervisão (S), Proteção (P), Controle (C)

- **3. Vetor e Pré-condição do Ataque**
  Vetor de ataque: Um atacante com conhecimento prévio da rede e de suas configurações consegue acesso físico a uma porta trunk do switch de processo. Explora configurações inseguras de controle de acesso, ausência de mecanismos de autenticação, falta de monitoramento de dispositivos não autorizados e segmentação inadequada da rede (uso de VLANs), sendo capaz de injetar frames SMV/GOOSE malformadas.
- **4. Procedimento de Teste**
  Equipamentos de Teste: Conprove CE-MNET (injeção de frames malformadas)
- Descrição da Conexão:
  O CE-MNET conecta-se a uma porta trunk do switch de processo.

- Configuração de Rede:
  Porta trunk do switch de processo com acesso às VLANs de processo. Utiliza-se endereçamento multicast correto para os protocolos GOOSE e SMV.
- Descrição da Execução:
  O CE-MNET fabrica e injeta frames cortados com campos faltantes direcionadas aos IEDs e MUs do barramento de processo. O objetivo é verificar a operação do IED e que não haverá reinicializações, travamentos ou comportamento imprevisível.
- Objetivos:
  • Demonstrar que não há qualquer comportamento inesperado do sistema

- **Subcenários de Execução**

- **Sc6-A — GOOSE Malformado de IED para MU**
  O CE-MNET fabrica frames GOOSE com campos malformados simulando a origem de um IED. Os frames são direcionadas à MU.

- **Sc6-B — SMV Malformado de MU para IED**
  O CE-MNET fabrica frames SMV com campos malformados simulando a origem de uma MU. Os frames são direcionadas ao IED.

- **5. Resultados Esperados**

  Sem Mitigação: Não travamentos ou resets inesperados do IED

- **6. Métodos de Detecção e Monitoramento**

  Ferramentas: CONPROVE e WEG

- **7. Medidas de Mitigação**

  Firmwares dos IEDs já resilientes ao ataque.

SIEMENS

Sc7 · Flooding SMV — Saturação do Barramento de Processo

Barramento de Processo | Nível de Automação: Processo | Impacto: Alto

- **1. Identificação do Ataque**

  Tipo de Ataque: [INJECTION] / [Fabrication] / [DoS]

  Nível de Automação: Processo

  Alcance / Nível de Impacto: Alto — Supervisão (S), Proteção (P), Controle (C)

- **2. Alcance e Objetivo**

  Nó / Ativo Alvo: IEDs de baia, switch do Barramento de Processo

  Função Alvo (SPAC): Supervisão (S), Proteção (P), Controle (C)

- **3. Vetor e Pré-condição do Ataque**
  Vetor de ataque: Um atacante com conhecimento prévio da rede e de suas configurações consegue acesso físico a uma porta trunk do switch de processo. Explora configurações inseguras de controle de acesso, ausência de mecanismos de autenticação, falta de monitoramento de dispositivos não autorizados e segmentação inadequada da rede (física e VLANs).
- É capaz de injetar fluxos SMV capazes de saturar a largura de banda do barramento ou a capacidade de processamento dos dispositivos, gerando uma negação de serviço.
- **4. Procedimento de Teste**
  Equipamentos de Teste: Conprove CE-MNET (geração massiva de fluxos SMV)

- Descrição da Conexão:
  O CE-MNET conecta-se a uma porta trunk do switch de processo.
- Configuração de Rede:
  Porta do switch de processo com acesso às VLANs de processo. Utiliza-se o endereço MAC multicast correto para os fluxos SMV.
- Descrição da Execução:
  O CE-MNET gera simultaneamente 60 ou mais fluxos SMV artificiais direcionados ao IED de bay, utilizando o endereçamento MAC multicast correto para que os fluxos sejam processados pelo switch e não descartados na camada L2. O volume de tráfego SMV gerado satura a largura de banda do barramento de processo e/ou o processador dos dispositivos, causando perda de pacotes nos fluxos SMV legítimos e eventual indisponibilidade do barramento.

- Objetivo (VERIFICAR):
  - Confundir a medição do supervisório e bloquear a função de proteção 87L

- **5. Resultados Esperados**
  Sem Mitigação: Comprometimento da disponibilidade — perda das funções de supervisão, proteção e controle devido à indisponibilidade do barramento de processo.

- **6. Métodos de Detecção e Monitoramento**
  Ferramentas: CONPROVE e WEG

- **7. Medidas de Mitigação**
  SIEMENS

Sc8 · Flooding SMV — Saturação do Barramento de Estação

Barramento de Estação | Nível de Automação: Estação | Impacto: Alto

- **1. Identificação do Ataque**
  Tipo de Ataque: [INJECTION] / [Fabrication] / [DoS]
  Nível de Automação: Estação
  Alcance / Nível de Impacto: Alto — Supervisão (S), Proteção (P), Controle (C)

- **2. Alcance e Objetivo**
  Nó / Ativo Alvo: IEDs de baia, switch do Barramento de Estação
  Função Alvo (SPAC): Supervisão (S), Controle (C)

- **3. Vetor e Pré-condição do Ataque**
  Vetor de ataque: Um atacante com conhecimento prévio da rede e de suas configurações consegue acesso físico a uma porta do switch de estação. Explora configurações inseguras de controle de acesso, ausência de mecanismos de autenticação, falta de monitoramento de dispositivos não autorizados e segmentação inadequada da rede.

- Com isso, por meio da configuração de uma porta trunk com acesso às VLANs, é capaz de injetar fluxos SMV capazes de saturar a largura de banda do barramento, gerando uma negação de serviço.

- **4. Procedimento de Teste**
  Equipamentos de Teste: Conprove CE-MNET (geração massiva de fluxos SMV)

- Descrição da Conexão:
  O CE-MNET conecta-se a uma porta trunk do switch de estação.
- Configuração de Rede:
  Porta do switch de estação com acesso às VLANs de estação. Utiliza-se o endereço MAC multicast correto para os fluxos SMV.
- Descrição da Execução:
  O CE-MNET gera simultaneamente 20 ou mais fluxos SMV artificiais direcionados ao IED de bay, utilizando o endereçamento MAC multicast correto para que os fluxos sejam processados pelo switch e não descartados na camada L2. O volume de tráfego SMV gerado satura a largura de banda do barramento de estação e/ou o processador dos dispositivos, causando falha na comunicação e eventual indisponibilidade do barramento (mensagens SMV tem maior prioridade).

- **Objetivo** (VERIFICAR):
  - Confundir a medição do supervisório

- **5. Resultados Esperados**
  Sem Mitigação: Comprometimento da disponibilidade — perda das funções de supervisão e controle devido à indisponibilidade do barramento de estação.

- **6. Métodos de Detecção e Monitoramento**
  Ferramentas: CONPROVE e WEG

- **7. Medidas de Mitigação**
  SIEMENS

ORGANIZA cigre Paraguay

APOYA ITAIPU BINACIONAL

CONPROVE

weg

SIEMENS

Belden

GRACIAS!!!