Teoretický systémový přístup k bezpečnostním hrozbám kyberfyzikálních systémů aplikovaný na Stuxnet

Bc. Lukáš Pelánek

Úvod

- Kvůli problémům jako nedostatek energie je potřebná integrace výpočetní techniky do fyzického světa.
- Útoky na CPS (Kyberfyzikální systémy) mohou způsobit i národní pohromy - u takových systémů je třeba zajistit dokonalé zabezpečení během všech fyzických i kybernetických procesů.
- CPS nemusí být jakkoliv propojeny s okolním kyberprostorem, aby se staly zranitelnými.
- Ve většině případů se hledí především na zabezpečení CPS na úrovni komponent (každý prvek systému izolovaný), což není dostatečné.

Kyberfyzikální systémy (CPS)

- Jde o systémy, jenž umožňují ovládání fyzických komponent počítačovými příkazy.
- Díky řídícím jednotkám, senzorům a komunikačním jádrům vytvoří CPS řídící smyčku pro každou fyzickou součást systému.
- Hlavními komponenty CPS jsou:
  - **SCADA** - supervisory control and data acquisition,
  - **DCS** - distributed control system,
  - **PLC** - program logic controller

Metody analýzy zabezpečení v CPS

- Žádné z tradičních metod (**FTA**, **FMEA**, **HACCP**, **HAZOP**) nepočítají s hrozbami, které zneužívají interakcí jednotlivých komponent CPS.
- Narozdíl od nich nový model **STAMP** (Systems Theoretic Accident Model and Process) nepovažuje bezpečnost za problém spolehlivosti a je navržen pro komplexní systémy s mnoha komponenty, jako například právě CPS.

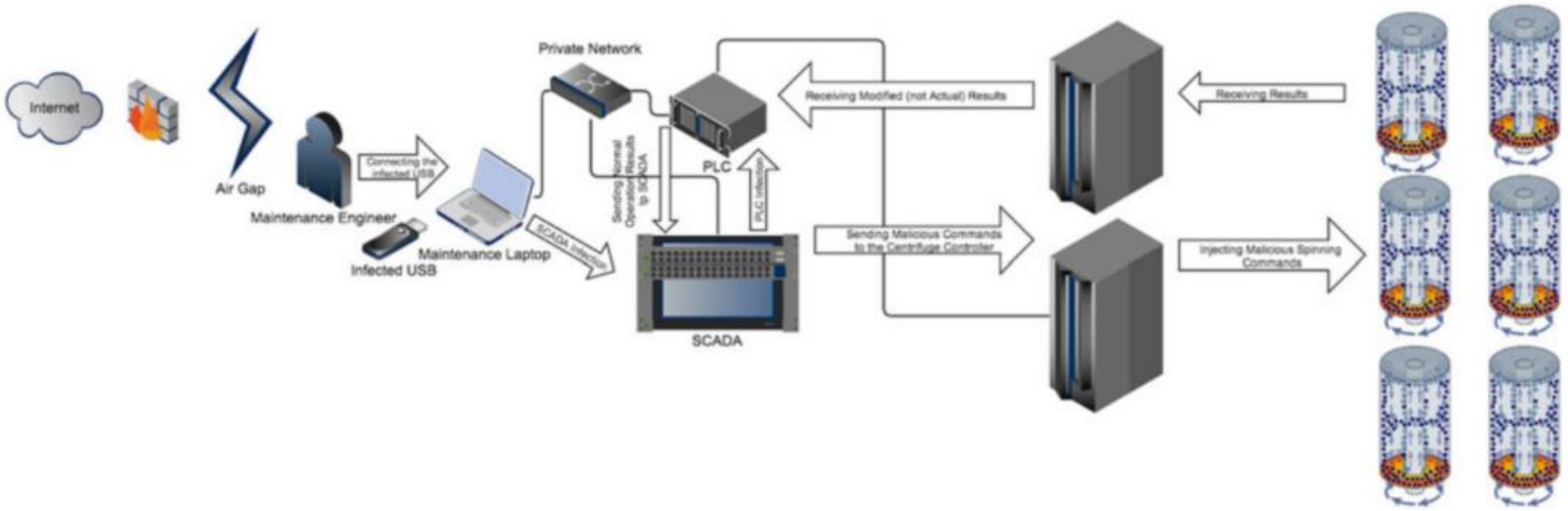
System Theoretical accident Mode and Processes (STAMP)

- Je novým způsobem myšlení o nehodách, který integruje všechny aspekty rizika, včetně organizačních a sociálních aspektů.
- Aspekt tohoto přístupu k managementu rizika je důraz na použití vizualizace a tvorbu sdílených mentálních modelů komplexního systémového chování.

Případ Stuxnet

- Poprvé objeven společností VirusBlockAda v červnu 2010, nakazil počítače po celém světě (většina z nich se nacházela v Íránu).
- Velmi komplexní a pečlivě zaměřený (nepoškodil jiná infikovaná zařízení pro obohacování uranu), byl pravděpodobně testován na podobné architektuře elektrárny.
- Jde pravděpodobně o největší útok na CPS.
- Útočil na PLC, k jejichž dokumentaci měli autoři útoku pravděpodobně přístup.

Stuxnet attack diagram



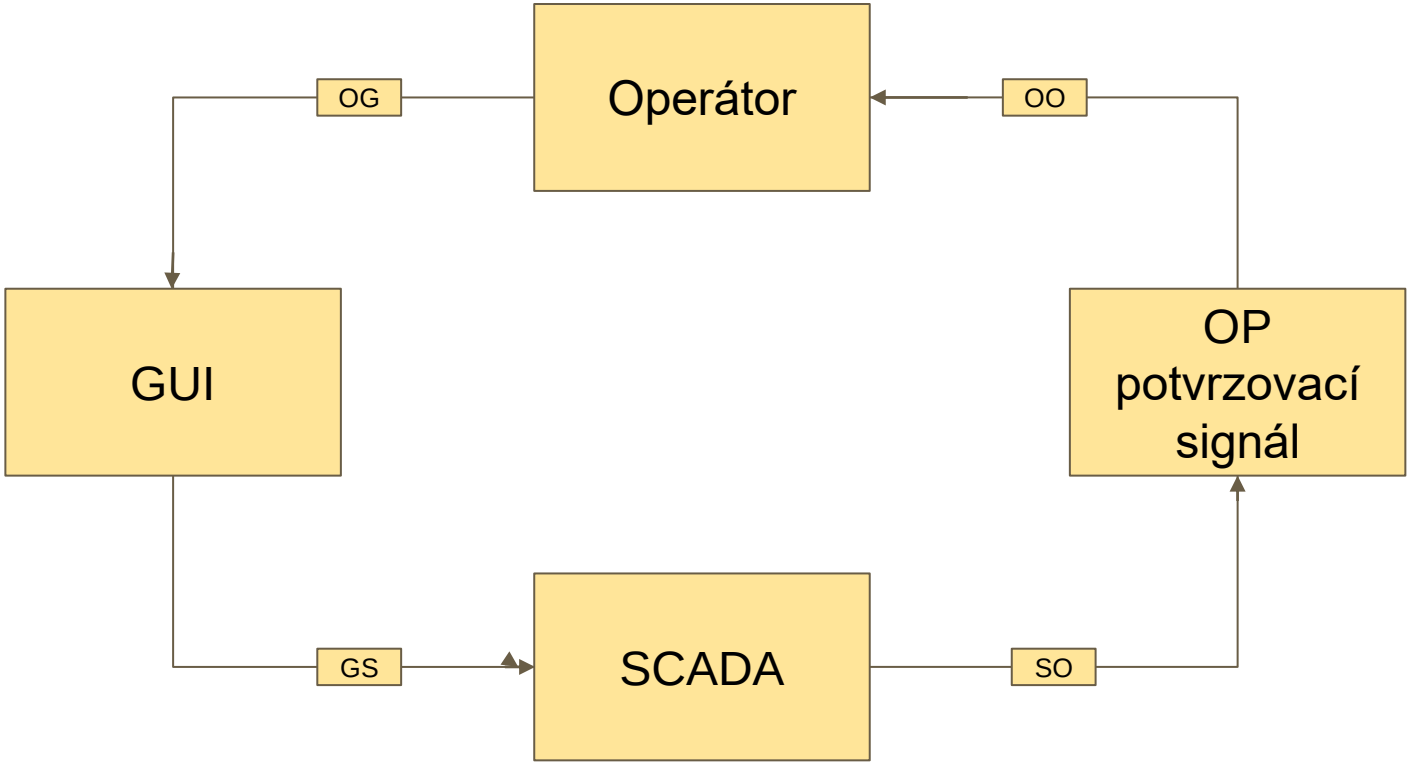
Analýza infekce Stuxnet

- Infikována byla všechna zařízení v síti vč. těch nejdůležitějších komponent (SCADA, čtečky senzorů...)
- Infekce byla úzce zaměřená na produkty Siemens S7/WinCC.
- Pro získání root přístupu a manipulaci s PLC byly zneužity 3 zero-day zranitelnosti systému Windows:
  - částečně neopravená zranitelnost Conficker,
  - neošetřená práce s odkazy (*.LNK soubory),
  - chyba ve službe Print Spooler využita pro rozšíření zranitelnosti po síti
- Infikovány byla také např. všechny připojené USB disky a soubory projektů systému Siemens S7 pro ovládání PLC.

CAST analýza Stuxnetu

- Účelem této analýzy je zjistit, jestli by metodologie STAMP dokázala odhalit rizika vedoucí k selhání odstředivek v případě Stuxnet.
- CAST analyzuje každý komponent komplexního CPS a zohledňuje parametry jako příchozí data, jejich zdroje a interakce s ostatními komponenty funkčního systému.
- Každé toto spojení se označuje prvním písmenem názvu počátečního komponentu a komponentu na něj navazujícího.
- V případě Stuxnet byly interakce mezi operátory, SCADA systémy, PLC a senzory narušeny a chybějící autentizace a ověření výsledků umožnily spuštění škodlivých operací.

Řídící smyčka fyzikálních systémů (CAST)



Řídící struktura systému

- Systém lze rozdělit do 3 základních sub-systémů:
  - Operační (zahrnuje uživatelská rozhraní, řídící algoritmy, ověřovací systémy)
  - Řídící (zahrnuje SCADA, PLC, ovladače zařízení)
  - Komunikační (zahrnuje síťové komunikace mezi jednotlivými entitami systému)

Komponenta	**Odpovědnosti**
Fyzické koncové body	Příjem hodnot příkazů systému, provádění požadovaných operací, hlášení výsledků a stavu koncových bodů
Operátor	Hlavní uživatel systému -zadávání příkazů, tvorba protokolů a reakce na výstup systému
SCADA	Překlad příkazů operátora pro každou fyzickou komponentu a příprava výsledků pro kontrolu
Komunikační síť	Přenos informací mezi jednotlivými komponenty v síti
Monitorovací senzory	Monitoring výsledků akcí prováděných fyz. koncovými body a jejich nahlášení controlleru

Závěr

- Návrh zabezpečení pro kyberfyzikální systémy musí počítat s mnoha specifickými vlastnostmi takových systémů, jako např.:
  - interakce mezi kybernetickým a fyzickým prostředím,
  - distribuovaný management a řízení,
  - geografická distribuce
- Díky CAST analýze bylo zjištěno několik hrozeb, které ukazují na chybějící články návrhových požadavků, které byly potřebné v původním návrhu tohoto případu.

Zdroj

Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet, IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 1, January/February 2018

Autoři

Arash Nourian
MIT University

Stuart Madnick
MIT University