**Příloha ke Crypto-Worldu 4/2005 (PR)**

# SINA - BEZPEČNÁ KOMUNIKAČNÍ INFRASTRUKTURA

**Josef STRELEC,** Secunet, s.r.o. (strelec@secunet.cz)

**Abstrakt**

*Architektura Secure Inter-Network Architecture (SINA) umožňuje bezpečnou komunikaci v rámci virtuální privátní sítě (VPN) s IP šifrováním (layer 3). Je založena na mnoha komponentech, které jsou průběžně zdokonalovány a přizpůsobovány novým požadavkům.*

## 1. SECURE INTER NETWORK ARCHITECTURE

### 1.1 Co je SINA (Secure Inter-Network Architecture)


SINA je řešení, které umožňuje bezpečnou komunikaci počítačů připojených do sítě. Tento systém je založen na principu vytváření šifrovaných tunelů (VPN) mezi jednotlivými komunikujícími počítači či LAN. SINA ale není jen IP šifrátor. Architektura SINA se skládá z několika průběžně rozšiřovaných produktů, které v sobě integrují níže uvedené vlastnosti. SINA je navíc podporována technologií čipových karet a kompletní PKI.

### 1.2 Původ SINA

SINA vznikla pod záštitou německé státní organizace BSI (Bundesamt für Sicherheit in der Informationstechnik) ve spolupráci s firmou **secunet**.

### 1.3 Certifikáty SINA

Architektura SINA byla schválena **Spolkovým úřadem pro bezpečnost informačních technologií** (BSI) jako vhodná pro přenos utajovaných informací až po bezpečnostní klasifikaci **TOP SECRET** (PŘÍSNĚ TAJNÉ) – což je v případě řešení založeného na internetovém protokolu unikátní. Řešení SINA obdrželo od **NATO** v roce 2003 certifikaci pro přenos klasifikovaných informací do stupně „**NATO-SECRET**“. V lednu 2005 získalo řešení SINA Box S certifikát pro přenos klasifikovaných informací EU na stupeň **CONFIDENTIAL EU** včetně. Probíhá certifikace **Národním bezpečnostním úřadem** České republiky na stupeň utajení TAJNÉ.

### 1.4 Průmyslové standardy

Architektura SINA vyhovuje standardu **IPSec**, RFC 2401-2412. Z dalších implementovaných standardů různých rozhraní implementovaných v řešení SINA dále uvádíme RFC 1777 (LDAPv2), RFC 2104 (HMAC), RFC 2367 (PFKey), RFC 2459 (X509v3), RFC 2510/2511 (CMP) či ISO IEC 15946-2 (EC-GDSA).

Pro řešení vzdálených individuální uživatelů, kteří by mohli být vybaveni řešením SINA-Think-Client (terminálový klient), jsou implementovány protokoly RDP (Microsoft), ICA (Citrix) a X11.

## 1.5 Kdo SINA používá

SINA je používána všude tam, kde jsou kladeny vysoké nároky na zajištění bezpečnosti. Nejlepším příkladem je německé ministerstvo zahraničních věcí, které používá SINA k zabezpečení komunikace se svými zastupitelskými úřady.

## 1.6 Vlastnosti SINA

**Vysoká bezpečnost**

- Na rozdíl od komerčně dostupných řešení je SINA postavena s použitím tzv. „Open source software“, což znamená, že zdrojový kód je plně pod kontrolou veřejnosti. Lze tedy auditovat řešení proti zabudování „zadních vrátek“, která se mohou teoreticky v proprietárních řešeních nacházet.
- Autentizace uživatele je prováděna pomocí čipových karet, které lze generovat v integrované infrastruktuře PKI.
- Použití technologie PKI včetně elektronického podpisu zaručuje důvěryhodnost přenášených dat. Technologie čipových karet zamezuje zneužití systému neoprávněnou osobou.


- Architektura je dále vybavena funkcemi směrování a subsystémem pro detekci napadení a reakci na ně.
- V řešení SINA jsou implementovány různé krypto algoritmy. A to buď softwarové a nebo pro vyšší stupně utajení hardwarové. Hardwarové algoritmy jsou implementovány prostřednictvím krypto čipu na speciální PCI kartě, která je vložena do PC, na kterém běží SINA. Všechny šifrovací algoritmy jsou připojeny přes jednotné a otevřené API, což otevírá možnost na implementaci dalších algoritmů.

**Rozšiřitelnost**

Šetří finanční prostředky za nákup dalších technologií – SINA je možné použití pro šifrování hlasových přenosů (voice/IP) či videokonference.

**Flexibilita**

SINA nenutí zákazníka do používání výrobcem definovaných politik, ale umožňuje implementaci různých bezpečnostních nastavení. Z jedné stanice lze realizovat přístupy na různých úrovních bezpečnosti.

**Otevřenost**

Umožňuje implementaci různých kryptoalgoritmů. Volba kryptoalgoritmu je na zákazníkovi, SINA podporuje SW nebo i HW šifrování. Lze zvolit algoritmy implementované společností secunet (např. 3DES, AES) nebo zvolit národní (firemní) šifrovací algoritmus).

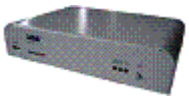
**Univerzální aplikovatelnost**

Architektura SINA využívá výhradně osvědčený standardní PC hardware, který je efektivní z hlediska nákladů a lze jej dodávat dlouhodobě. Architekturu je navíc možno integrovat do každé nižší IT infrastruktury založené na protokolu IP. Rozhraní podporuje sítě 10/100/1000 Mbit (TX/FX), s rozhraními WaweLAN (802.11b), token ring, PPP, PoE.

**Škálovatelnost**

Architektura SINA je v současnosti představována následujícími produkty:

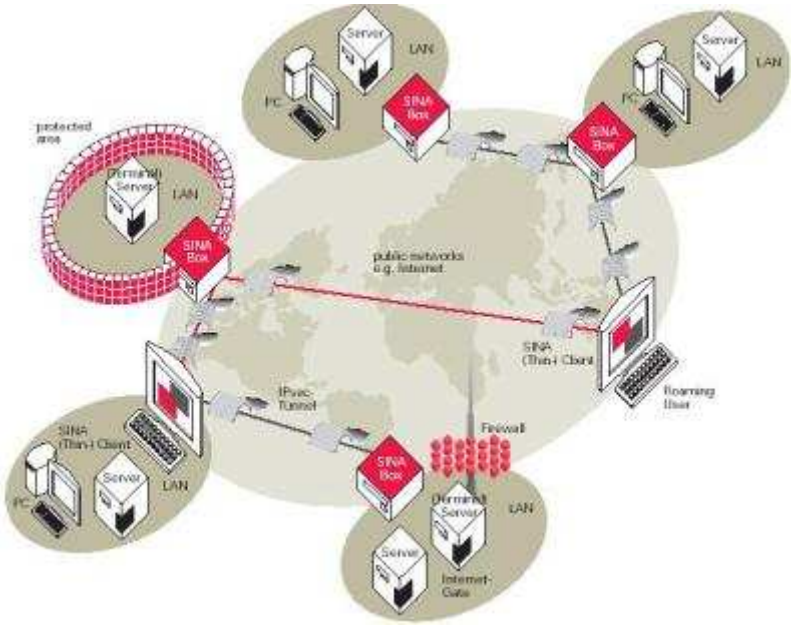
- SINA-box (minimalizovaný a zodolněný SINA-Linux, portace na standardní „Intel based“ PC nebo tempestované PC, zavádění systému z CD-ROM, volitelný šifrovací algoritmus, konfigurace na čipové kartě).
- SINA-Thin-Client (klient pro terminálový server, žádné ukládání senzitivních dat, řízený přístup prostřednictvím čipových karet pro přístup k informacím s různou úrovní informační bezpečnosti – v jednom okamžiku lze mít až 6 terminálových sessions k různým terminálovým serverům (RDP, ICA, X11)).
- SINA-Cluster (řešení pro dosažení vysokého výkonu a dostupnosti, dosažení propustnosti systému až 400 Mbit/sec).
- SINA-Virtual-Workstation (plnohodnotná pracovní stanice, hostování např. MS Windows jako virtual machine pod operačním systémem LINUX).
- SINA Management Console – komplexní „all-in-one“ řešení pro management SINA architektury. SINA Management Console umožňuje definování bezpečnostních politik pro jednotlivé kryptografické prostředky. Zároveň umožňuje vydefinování bezpečnostních pravidel a to jak na úrovni sdílení celého rozsahu sítě, nebo jednotlivých IP adres až po vydefinování přístupu na konkrétní IP adresy, případně konkrétní port (porty). Databáze bezpečnostních politik je vytvořena po analýze potřeb a nastavení pravidel komunikace. Tato databáze musí respektovat bezpečnostní politiku. Mezi další komponenty Management Console patří např. PKI, CA, SQL databáze pro logování, atd.



**Vysoká výkonnost**

Přenosová výkonnost je škálovatelná v rozsahu od 40 do 400 Mbit/sec (např. při použití algoritmu AES (192 bit) na Pentium IV 2.4 GHz lze dosáhnout až 90 Mbit/sec).

**Praktický příklad architektury SINA**




Pro případ bezpečné komunikace dvou nebo více LAN jsou nutné pouze SINA-Boxy umístěné na vstupu nebo výstupu do LAN. Názorněji to demonstruje následující obrázek.

SINA řešení vytváří „bezpečnostní“ vrstvu nad komunikační infrastrukturou (dále jen KI). Z pohledu SINA je KI považována jako „nebezpečné“ prostředí a veškerá komunikace přes KI (WAN) je tedy šifrována. Nad touto infrastrukturou je možno vybudovat prostřednictvím SINA bezpečné VPN. Pokud to umožňuje bezpečnostní politika aplikace, je možno nastavením různých politik VPN tunelů vytvářet VPN tunely s rozdílnými parametry (IPsec, šifra, ..) pro přenos utajovaných a neutajovaných skutečností.

SINA umožňuje nastavit různé šifrované „tunely“. Jejich počet není licenčně omezen, omezení je dáno pouze HW konfigurací (např. při 128 MB operační paměti je možno mít na jednom SINA boxu až 4 000 aktivních tunelů). Každý VPN tunel (security association) může mít jinou bezpečnostní politiku (tím se rozumí např. jiné nastavení parametrů IPsec, jiný šifrovací algoritmus, atd.).

Významnou je i možnost připojení **jednoho uživatele** k **několika informačním zdrojům** **s různou úrovní bezpečnosti** (terminálové připojení prostřednictvím SINA Thin Client).

Další podrobnosti lze nalézt na www.secunet.cz či www.bsi.de .

## 2. ZÁKLADNÍ PŘÍNOSY SINA

1. Kompletní řešení zabezpečené a certifikovatelné on-line komunikace (**plnohodnotná obousměrná on-line IP konektivita**).
2. Implementace SINA **nevyžaduje** jakékoliv zásahy do architektury informačních systémů (jako např. instalace VPN klientů na PC či aplikační servery) nebo zásahy do komunikační infrastruktury (transportní vrstva). IS nemusí řešit komunikační bezpečnost. Bezpečnost je pro uživatele a aplikace zcela transparentní.
3. Využití **jedné** přenosové infrastruktury pro řešení celé řady různých projektů – růstový potenciál (každý může mít při **jedné** technologii svoji virtuální **oddělenou síť**).
4. Informační bezpečnost komunikační infrastruktury je řešena jako zcela transparentní, tzn. je možno použít **libovolné SW** řešení (bezpečnost je nezávislá na typech současných, ale i budoucích aplikací) pro implementaci portálu, dokument management systému či archivu dokumentů nebo již hotová řešení – **ochrana již vynaložených investic**.
5. **Vynikající poměr cena/výkon** (jedna licence SINA bez technických prostředků je pod 3 000,- EUR).
6. **Neomezený počet VPN** šifrovaných tunelů a **počet koncových uživatelů** v SINA chráněné síti (omezení dáno pouze výkonností HW).
7. Jako vlastní přenosovou síť lze použít některou z již existujících sítí jako např. KIVS, resortní WAN či firemní WAN. SINA řeší bezpečnostní vrstvu nad touto přenosovou sítí.
8. Navrhované řešení **ověřeno** v několika rozsáhlých implementacích v SRN.
9. Možnost implementace v řádu **jednotek měsíců**.
10. **Souběžný přístup** do sítí (k informačním zdrojům) s **různou** úrovní informační bezpečnosti **z jednoho počítače** (SINA Thin Client).
11. Potenciál dalšího rozvoje (stejná infrastruktura použitelná např. pro **voice-over-IP, videokonference**, …).
12. Otevřenost architektury pro implementaci **národní šifry**.

secunet s.r.o.
Evropská 33d, 160 00 Praha 6
*tel*. 233 029 711, *fax* 233 029 739
secunet@secunet.cz
www.secunet.cz
www.secunet.com
www.bsi.de