Phalanx

DigitalExpert

DigitalExpert

Consulenze Informatiche

di Carloalberto Sartor
via Astichelli 14, 36031 Dueville (VI) - Italy

Web Site: www.digitalexpert.it
Email: info@digitalexpert.it

Systems – Networking – Software & Hardware Development
Special projects – Kanban Solutions
Training – InterTechnology Integrations
Monitoring Systems – Web Applications
*Maintenance – **Security** - Forensic*
Telecommunications - Elettropollution

Phalanx Framework

Experiences in diagnostics

For

Networks, Systems and Services

Phalanx, IDS & Security Solutions

Phalanx – Le funzionalita' IDS

Phalanx opera secondo il principio del

controllo pervasivo

Questa metodologia si basa su tecniche

convenzionali / “non convenzionali”

che agevolano il riconoscimento e la gestione delle problematiche di Intrusione e di Sicurezza informatica

Phalanx – Il controllo pervasivo

Il controllo pervasivo delle intrusioni e' reso possibile dalla struttura polifunzionale di Phalanx, in grado di controllare separatamente e contestualmente I seguenti oggetti:

- **Phalanx Light** e' un modulo apposito costruito per veloci ed esaurienti analisi rapide volte ad identificare specifiche condizioni critiche di degrado di ambienti operanti su Ethernet e TCP/IP

- **Phalanx Toolkit** si interfaccia con tutti i dispositivi dotati di protocollo SNMP ricavando informazioni diagnostiche e prestazionali, siano essi locali o remoti

- **Phalanx Console** permette di attivare monitoraggi specifici oltre a implementare la funzione di Manager Phalanx (controparte degli agenti installati sui nodi)

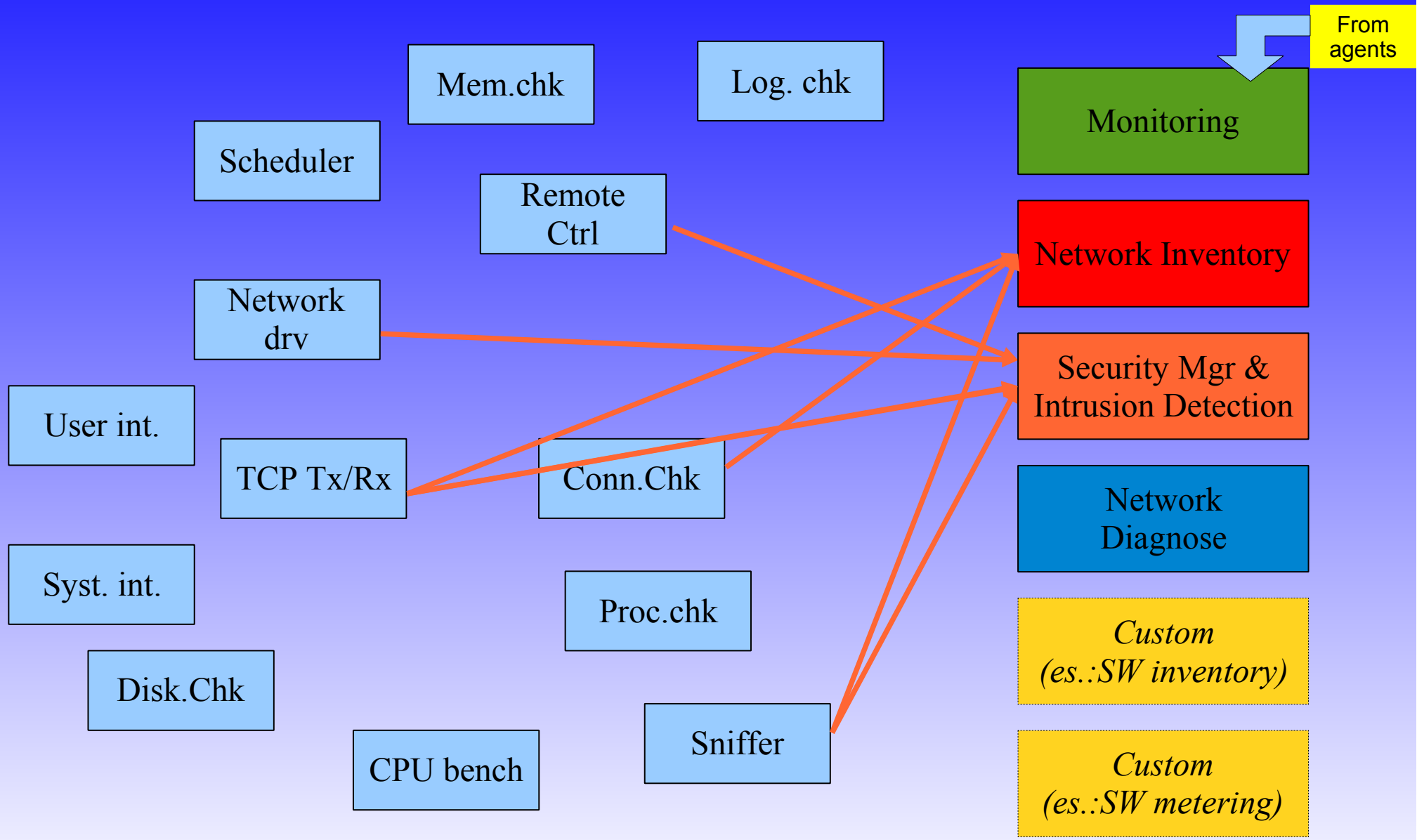
Phalanx – Il controllo pervasivo

Il controllo pervasivo delle intrusioni e' reso possibile dalla struttura polifunzionale di Phalanx, in grado di controllare separatamente e contestualmente i seguenti oggetti:

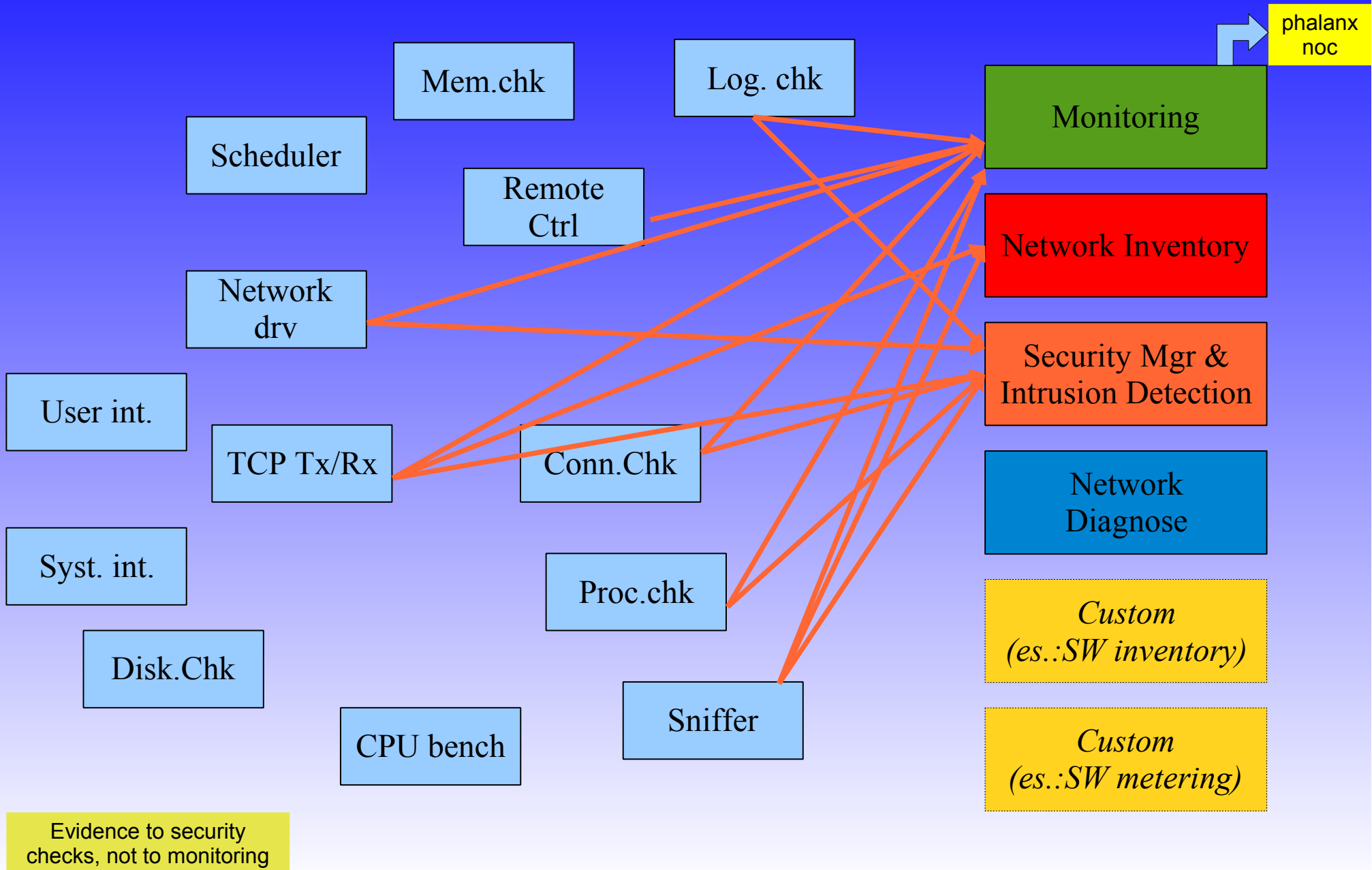
- **Rete:** inventario dei nodi, inventario dei servizi erogati, inventario dei protocolli circolanti, inventario delle sessioni in-out, inventario degli apparati, inventario dei best-talker e dei best-receivers, inevntario dei mac-address (fisici, logici, virtuali, broadcast, multicast), etc (tramite NOC)

- **Nodi:** inventari relativi a servizi erogati/utilizzati, sessioni attive/dead, applicazioni, connessioni applicazioni-nodi, inventario nodi connessi, composizione del traffico, nodi loggati, user behaviour, esame del contesto di rete
(tramite agenti e manager Phalanx)

Phalanx IDS – NOC scheme



Phalanx IDS – Agent scheme



Phalanx

Mainstream 1

Inventory di rete

Elenco interfaccie di rete e relative funzionalita' “normalmente attive” con evidenza di modifiche strutturali e comportamentali significative

(storicizzazione dei delta)

Phalanx

Mainstream 2

Analisi del traffico di rete

L'analisi del traffico identifica anomalie di:

- Composizione
- Distribuzione
- Frequenza
- Combinazione
- Contenuto
- Sorgenti e destinatari

(black/whitelist di indirizzi, porte, protocolli, contenuti)

Phalanx

Mainstream 3

Diagnostico di rete

Permette la misura dello stato delle interfaccie e di eventuali situazioni anomale dal punto di vista prestazionale o inventariale complessivo (protocolli, servizi, etc)

“C'e' un pc infetto che mi blocca la rete?
C'e' un cavo difettoso che causa problemi?”

Misuriamo!!!

Phalanx

Mainstream 4

User Behaviour analyzer

Verifiche effettuate tramite agenti permettono di inventariare le specifiche funzionalita' usufruite/erogate da uno specifico nodo (client o server), permettendo di evidenziare anomalie operative, classico sintomo di una intrusione.

Phalanx

Mainstream 5

Analizzatore del servizio erogato

Il controllo costante dei servizi erogati
(composizione, distribuzione temporale, destinatari)
permette di riconoscere accessi non desiderati ai server

La registrazione costante di questi elementi permette la ricostruzione di incidenti di sicurezza o verifiche comportamentali.

Phalanx

Mainstream 6

Analisi dei tempi di risposta WAN

Intrusione vuol dire anche “export” di dati e funzioni aziendali

Il coinvolgimento della connettivita' e' quindi un ulteriore elemento distintivo di eventuali intrusioni

L'accesso a consistenti risorse aziendali per l'alienazione massiva ha come punto nevralgico la connettivita', la quale si trova ad essere coinvolta in una operazione sicuramente anomala.

Ecco che il controllo e la registrazione costante degli impegni di connettivita' permette di identificare e ricostruire eventuali problematiche di questo tipo, diversamente silenti.

Phalanx

Mainstream 7

Controllo configurazione di firewall

E' evidente che la strumentazione di governo della sicurezza costituisce un punto critico e spesso oggetto di “attacchi” volti a modificarne la configurazione o ad avvalersi di “buchi” non documentati.

L'analisi della configurazione del firewall e la verifica del suo comportamento effettivamente “bloccante” sugli aspetti vitali dell'infrastruttura informatica permette di evidenziare criticita', guasti, comportamenti imprevisti, configurazioni errate, accessi illeciti.

Phalanx

Mainstream 8

Network Context Control

L'analisi del contesto di rete permette di evidenziare anomalie di composizione del mondo circostante (ad esempio 'mac address neighbour', protocolli circolanti, nomi di rete, servizi di rete caratteristici, indirizzi, domini, caratteristiche della connettivita' pubblica, etc)

Phalanx

Mainstream 9

Service Mapper

Il service mapper permette di verificare molto rapidamente se la composizione dei servizi disponibili nella rete del cliente e' diversa dal solito.

Il controllo effettuato dall'interno della LAN, coniugato al controllo effettuato sulla connettivita' pubblica permette di evitare l'esposizione non controllata di servizi erogati, quale che sia la causa scatenante.

Phalanx

Mainstream 10

User Access Log

Il controllo dei logins e degli accessi (e la relativa storicizzazione) permette di identificare e storicizzare ogni eventuale acceso indesiderato, quale che sia l'origine di esso

(malintenzionati, errate configurazioni, errori degli utenti, applicazioni vecchie, etc)

Phalanx

LINEA 15 - bis

Administrator Access Log

(un sottoprodotto dello User Access Log)

(vedi "Tracciatura Accessi Amministrativi" - Privacy)

Provvedimento “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”

27 novembre 2008 - G.U. n. 300 del 24 dicembre 2008

IN VIGORE DAL 15 DICEMBRE 2009...

Phalanx

Mainstream 11

Building Local Healt Manager

Il controllo complessivo della strutturazione del building (interfaccie, apparati, composizione, numero di nodi presenti) permette una agevole identificazione di eventuali connessioni fisiche indesiderate od intromissioni nella struttura di rete.

Phalanx

Mainstream 12

Software Metering

La rilevazione costante di programmi e servizi utilizzati su clients e server permette di identificare oggetti software non conosciuti che vengano attivati all'interno della rete aziendale.

Cio' permette di riconoscere eventuali intromissioni (dolose, accidentali) quale che sia l'origine di esse.

Il contributo di questo strumento al controllo generale della sicurezza aziendale e' sicuramente fondamentale, in quanto la caratteristica di scarso controllo del software utilizzato e' all'origine di numerose problematiche di sicurezza (oltre che di licenza e di capacity)

Phalanx

Mainstream 13

Tools specifici di diagnosi commandline!

Il framework Phalanx permette la realizzazione di specifici tools commandline, anche utilizzabili al di fuori dello specifico ambito di Phalanx, in grado di identificare specifici strumenti di intrusione o specifiche criticita'.

Phalanx

Mainstream 14

Servizio “localizzazione IP” / Antifurto

Il sempre maggiore utilizzo di sistemi “mobile” per l'accesso ai servizi aziendali, ha suggerito l'implementazione di meccanismi di identificazione dei sistemi connessi dal mondo esterno.

Questi meccanismi permettono da una parte una mutua validazione dell'accesso, attraverso una identificazione pervasiva del sistema connesso, riconosciuto e inventariato in azienda per varie caratteristiche. Dall'altra il sistema oggetto di furto che venisse utilizzato per connettersi alle risorse aziendali viene identificato (quando, da che IP, azioni svolte, connessioni effettuate), garantendo la migliore sicurezza aziendale e registrazione delle azioni compiute.

Phalanx

Mainstream 15

Gestione ambienti “misti”

Non e' raro che una rete aziendale fisica contenga sistemi di clienti diversi. Questo aspetto, spesso oggetto di gestione complementare di partners diversi, puo' essere supervisionato a livello di sicurezza in modo centralizzato tramite un NOC.

L'inventario complessivo viene ripartito “per azienda” con un'area di segnalazione di oggetti che non sono in carico ad alcuno.

DigitalExpert

Consulenze Informatiche

di Carloalberto Sartor
via Astichelli 14, 36031 Dueville (VI) - Italy

Web Site: www.digitalexpert.it
Email: info@digitalexpert.it

Grazie per l'attenzione!

Fine