Indice

1. NUOVO COMITATO DIRETTIVO DEL CLUSIT

Nel corso dell'assemblea generale del 15 dicembre, si è proceduto all'elezione del nuovo Comitato Direttivo e del suo Presidente, che resteranno in carica fino al 31.12.2010. Sono stati eletti: Gigi Tagliapietra (Presidente), Luca Bechelli, Bruno Carbone, Raoul Chiesa, Mauro Cicognini, Gabriele Faggioli, Mariangela Fagnani, Giorgio Giudice, Paolo Giudice, Massimiliano Manzetti, Marco Misitano, Mattia Monga, Alessio Pennasilico, Stefano Quintarelli e Claudio Telmon.

2. SEMINARI CLUSIT EDUCATION NEL 2009

Il calendario 2009 dei seminari Clusit Education, riservati ai soci, è disponibile all'indirizzo www.clusit.it/clusit_edu_2009.pdf.

Ringraziamo i nostri sponsor, che ci hanno permesso di mettere a punto un programma particolarmente ricco: oltre a Confindustria Servizi Innovativi e Tecnologici, Lampertz Italia e la società Percorsi, quest'anno si sono aggiunti Oracle Community e Rittal SpA

3. CERTIFICAZIONI CISSP E CSSLP

Per il 2009 il Clusit ha ampliato il panorama delle certificazione professionali, offrendo nel calendario di seminari ed esami anche la nuova certificazione CSSLP (Certified Secure Software Lifecycle Professional) che (ISC)² propone per i professionisti della sicurezza del software, considerata lungo tutto il ciclo vitale.

Le date di seminari ed esami previste nel 2009 dal Clusit come (ISC)² Education Affiliate Authorized Provider sono:

Milano	4 - 8 maggio 2009	Seminario di preparazione all'esame **CISSP**
Monza	11 - 15 maggio 2009	Seminario di preparazione all'esame **CSSLP**
Monza	13 giugno 2009	**Esami (ISC)²**
Roma	19 - 23 ottobre 2009	Seminario di preparazione all'esame **CISSP**
Roma	21 novembre 2009	**Esami (ISC)²**

Le informazioni sulle certificazioni (ISC)² sono su www.clusit.it/isc2 e www.isc2.org o scrivendo a isc2@clusit.it

4. SECURITY SUMMIT 2009

Ecco un' anteprima di alcuni momenti di formazione ed altri eventi che si terranno nell'ambito del Security Summit di Milano dal 24 al 26 marzo.

Nel corso del mese di gennaio tutti i dettagli sull'intero programma del Summit e sui keynote, docenti e relatori, saranno pubblicati su www.securitysummit.it

Riportiamo le tematiche ed i nomi dei docenti dei tre percorsi formativi professionali:

Percorso Professionale "**TECNICO**"

1ª sessione - 24 marzo, 11.15/13.00

Le Botnet - prima parte

Docenti: Lorenzo Martignoni e Roberto Paleari

2ª sessione - 25 marzo, 11.15/13.00

Le Botnet - seconda parte

Docenti: Lorenzo Martignoni e Roberto Paleari

3ª sessione - 26 marzo, 11.15/13.00

Social Engineering

Raoul Chiesa e Andrea Ghirardini.

Percorso Professionale "**LEGALE**"

1ª sessione - 24 marzo, 11.15/13.00

La responsabilità amministrativa delle persone giuridiche nei delitti informatici

Docente: Gabriele Faggioli

2ª sessione - 25 marzo, 11.15/13.00

Data retention. Limiti e obblighi di legge

Docente: Giovanni Ziccardi

3ª sessione - 26 marzo 11.15/13.00

Il trattamento dei dati personali e le misure di sicurezza. Lo stato dell'arte normativo

Docente: Emilio Tosi.

Percorso Professionale "**GESTIONE DELLA SICUREZZA**"

1ª sessione - 24 marzo, 11.15/13.00

Gestione della sicurezza delle informazioni e certificazioni

Docente: Claude Maury

2ª sessione - 25 marzo, 11.15/13.00

Quali i prerequisiti per la scelta di un fornitore di servizi di Sicurezza Informatica

Docenti: Raoul chiesa, Pierluigi Perri, Luigi Vannutelli

3ª sessione - 26 marzo 11.15/13.00

Quali requisiti professionali sono necessarie per chi si occupa di sicurezza ICT in azienda

Docenti: Giorgio Giudice, Fabio Guasconi, Silvano Ongetta, Anthony Wright.

Inoltre si svolgerà un Corso Basico dal titolo **Introduzione alla sicurezza informatica**, rivolto a chiunque utilizza il sistema informatico o la rete in azienda. Il corso si terrà nell'arco di un'intera giornata e sarà replicato nei tre giorni. I docenti saranno: Luca Bechelli e Claudio Telmon. Per gli aspetti legali è prevista, ogni giorno, una sessione dal titolo **Il controllo nell'utilizzo delle strumentazioni informatiche e telematiche aziendali da parte dei collaboratori** ed i docenti saranno: Fabio Bravo, Pierluigi Perri e Giorgio Spedicato.

Segue il programma di due delle numerose Tavole Rotonde:

24 marzo - 14.30/17.30

Tavola Rotonda organizzata da ANSSAIF (Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria) sul tema:

L'attenzione delle banche alla Sicurezza del Cliente: da un approccio cost oriented alla creazione di valore.

Chairman: Anthony Cecil Wright, Presidente ANSSAIF.

Partecipano alla TR:

- Paolo Campobasso – Chief Security Officer Unicredit Group;
- Romain Defline, Group Compliance / Group Business Continuity – BNP Paribas, Parigi;
- Vincenzo Giardina, Responsabile Funzione Audit ICT, Servizio Internal Audit - Consorzio Operativo Gruppo MPS;
- Paola Guerra Anfossi – docente percorso Criminalità e Sicurezza Università Cattolica del Sacro Cuore di Milano;
- Massimiliano Magi Spinetti - ABI – Vice Presidente ABILab;
- Marina Monferino – Responsabile Sicurezza Dipartimento ICT - Banca Popolare di Milano;
- Leonardo Procopio - consigliere ANSSAIF;
- Anna Ryolo, Head of Organization, BCP Manager - BNP Paribas, Milano.

Obiettivo della TR:

Il cittadino avverte l'importanza dell'accesso ai canali informativi e dispositivi, via ATM e Web, offerti dagli intermediari finanziari, ma, allo stesso tempo, viene informato quotidianamente di frodi perpetrate da una criminalità sempre più agguerrita.

Il cittadino si accorge altresì che le banche adottano sistemi di sicurezza e comunicazioni estremamente differenziati, che lo disorientano.

Inoltre, l'attuale turbolenza dei mercati e la recessione oramai estesa a tutte le Nazioni più rilevanti, lo preoccupa sotto il profilo della previsione di investimenti in Sicurezza che le banche vorranno affrontare nei prossimi mesi.

Il cittadino non sa però che gli esperti di sicurezza in banca si incontrano, sempre più spesso, per discutere di questi ed altri problemi, quali la continuità del servizio e la gestione di gravi emergenze. Si possono citare, a titolo di esempio, i gruppi di lavoro presso l'ABI, l' ANSSAIF e, non ultima, la recente esperienza di oltre 50 esperti di sicurezza a Bologna, di cui verranno illustrate sinteticamente le risultanze.

La tavola rotonda si pone pertanto l'obiettivo di rispondere agli interrogativi citati e a quelli che perverranno dalla sala.

25 marzo - 14.30/17.30

Tavola Rotonda che metterà a confronto le esperienze dei CSO di alcune delle più importanto aziende italiane sui temi:

Convergenza fra sicurezza fisica e sicurezza logica" e "Protezione delle infrastrutture critiche.

Chairman: Alessandro Lega - Senior Security Consultant - CPP ASIS International.

Partecipano alla TR:

- Paolo Campobasso – Chief Security Officer Unicredit Group.
- Franco Fiumara - Responsabile della Direzione Protezione Aziendale del Gruppo Ferrovie dello Stato;
- Stefano Grassi - Direttore della Struttura Tutela Aziendale di Poste Italiane
- Giuseppe Lasco - Responsabile Sicurezza Aziendale di TERNA
- Umberto Saccone - Responsabile Sicurezza Aziendale di ENI
- Damiano Toselli - Responsabile Sicurezza di Telecom Italia
- Domenico Vulpiani - Direttore del Servizio Polizia Postale e delle Comunicazioni.

Vi ricordiamo che, nell'ambito del Security-Summit di Milano, viene organizzata un'iniziativa che consente a singoli utenti e/o organizzazioni non commerciali quali Università, gruppi di interesse, gruppi di ricerca, di presentare nell'ambito della sicurezza informatica idee, progetti o prototipi non ancora sfruttati commercialmente. IL 30 GENNAIO SCADE IL TERMINE per rispondere alla Call For Paper www.clusit.it/securitysummit09/cfp_080927.pdf.

5. LA PROPOSTA SCHNEIER ALLA CALL DEL NIST

Il termine per la presentazione delle domande di partecipazione alla call del NIST http://csrc.nist.gov/groups/ST/hash/sha-3/index.html per l'individuazione di una nuova famiglia di algoritmi di hash è scaduto lo scorso 31 ottobre.

I contributi presentati http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo sono stati 64 (27 dei quali di pubblico dominio al momento, ndr) e sono decisamente tanti se confrontati con l'ultima call che vide la nascita di AES nel 1998 in cui le proposte furono solamente 16. Singolare che in entrambi i casi il numero delle proposte sia proprio una potenza di 2. Inoltre, alcuni sono stati già definiti "broken" ad una prima criptanalisi.

CI si aspetta adesso un periodo di qualche anno per la selezione dell'algoritmo "migliore" in cui i gruppi che hanno presentato la propria proposta effettuerà criptanalisi sul proprio e sull'altrui contributo. Questo periodo, estremamente importante per la selezione e rafforzamento delle proposte stesse, vedrà NIST da una parte e comunità crittografiche dall'altra apportare tutti quei contributi utili ad ordinare le proposte per funzionalità, efficienza, prestazioni e robustezza.

Per la parte finale del processo selettivo ci si aspetta pertanto di concentrarsi su un sottoinsieme di algoritmi particolarmente validi e completi.

Schneier e altri co-autori (Niels Ferguson, Stefan Lucks, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas e Jesse Walker) hanno presentato Skein www.schneier.com/skein.html.

Skein è una nuova famiglia di funzioni hash crittografiche. Il suo design unisce velocità, sicurezza, semplicità e una notevole flessibilità, il tutto all'interno di un package modulare facile da analizzare

Skein, scrivono gli autori, è veloce, sicuro, semplice, flessibile, efficiente e progettato da un team di esperti che hanno messo a fattor comune le loro esperienze.

Dall'executive summary una rapida overview.

Velocità
Skein-512 effettua l'hash dei dati a 6,1 cicli di clock per byte su una CPU a 64 bit. Ciò significa che con un processore Core 2 Duo x64 a 3,1 GHz Skein effettua l'hash dei dati a 500 MB al secondo per ciascun core – è quindi circa due volte più veloce di SHA-512 e tre volte più veloce di SHA-256. Una modalità hash-tree velocizza ancor di più le implementazioni parallelizzabili. Skein è veloce anche con i messaggi corti: Skein-512 effettua l'hash di messaggi corti in circa 1000 cicli di clock.

Sicurezza
Il suo design conservativo si basa sul block cipher Threefish. Al momento il nostro migliore attacco contro Threefish-512 è su 25 di 72 round, per un fattore di sicurezza di 2,9. Per fare un confronto, a uno stadio analogo del processo di standardizzazione, l'algoritmo di cifratura AES aveva un attacco su 6 di 10 round, per un fattore di sicurezza di 1,7 soltanto.

Semplicità
Utilizzando solamente tre operazioni primitive, la funzione di compressione di Skein può essere facilmente compresa e ricordata.

Flessibilità
Skein viene definito per tre dimensioni di stato interno (256 bit, 512 bit e 1024 bit), e per qualsiasi dimensione di output.

Un sistema di argomenti espandibile e completamente opzionale rende Skein uno strumento efficace da impiegare per un gran numero di funzioni: un PRNG (generatore di numeri pseudo-casuali), uno stream cipher, una funzione di derivazione di chiavi, autenticazione senza le informazioni addizionali del HMAC (Hashed Message Authentication Code), e la possibilità di personalizzazione.

Efficienza
Skein è efficiente su una grande varietà di piattaforme, sia hardware che software. Skein-512 può essere implementato in circa 200 byte di stato. Piccoli dispositivi, come le smart card a 8 bit, possono implementare Skein-256 utilizzando circa 100 byte di memoria. Dispositivi più grandi possono implementare le versioni maggiori di Skein per raggiungere velocità più elevate.

Le caratteristiche sulla carta sembrano esserci tutte.

Per gli addetti ai lavori ecco il paper: www.schneier.com/skein.pdf ed i sorgenti con test vector www.schneier.com/code/skein.zip.

Per gli altri, leggete, documentatevi e aspettate fiduciosi.

Autore: Armando Leotta

6. CYBERCRIME

Fra i più recenti attacchi di Ddos mossi da motivi politici troviamo quello contro il politico russo Gary Kasparov (ex grande scacchista e recentemente sentito all'evento SAP di Milano) e il suo partito nel corso della campagna per le elezioni russe . In questo caso, il sito www.theotherrussia.org è stato disattivato per un breve periodo di tempo, sufficiente però a impedirne l'uso da parte degli utenti interessati. Si è trattato di un attacco che non ha provocato danni significativi al partito politico, anche se ha voluto significare una rivolta e una protesta più che un tentativo di danneggiamento vero e proprio. Gli attacchi di stampo politico non si limitano alle reti russe ed europee. La maggior parte degli episodi che misuriamo con il nostro sistema Atlas proviene infatti dagli Stati Uniti ed è diretta a vittime statunitensi. In passato abbiamo assistito anche ad attacchi correlati ai conflitti indiani e pakistani, e di recente contro obiettivi iraniani.

Con l'aumento delle tensioni internazionali e con la sempre maggiore diffusione delle reti bot, prevediamo che la motivazione politica continuerà ad essere ampiamente utilizzata. Non crediamo che dietro a questo tipo di attacchi vi siano attività sponsorizzate da singoli governi, ma piuttosto semplici individui intenzionati a servirsi di Internet per esprimere le loro frustrazioni. Sarà a questo punto interessante vedere come gli eventi geopolitici si ripercuoteranno online nei prossimi mesi e anni. (Leggi l'articolo completo su www.eweekeurope.it/opinioni/gli-attacchi--ddos-sono-anche-di--natura-politica--9520).

Autore: Enzo M. Tieghi

Cyberattacco: dalla Russia con amore?

Segnaliamo un articolo apparso sul Los Angeles Times a proposito di un attacco informatico ai sistemi del Dipartimento della Difesa USA da parte, pare, di computer russi. Il condizionale è d'obbligo ma l'articolo è certamente una lettura interessante.

www.latimes.com/news/nationworld/iraq/complete/la-na-cyberattack28-2008nov28,0,230046.story

7. CAPTURE THE FLAG AL DEFCON 16: RESOCONTO FINALE

Nello scorso mese di giugno (vedi http://blog.clusit.it/sicuramente/2008/06/la-squadra-del.html) vi avevamo annunciato la probabile partecipazione della squadra dell'Università degli Studi di Milano (vedi http://security.dico.unimi.it) al "**Capture The Flag**" che si sarebbe tenuto al **DEFCON a Las Vegas**.

Oltre a Danilo Bruschi e Mattia Monga, che accompagnavano la squadra, hanno partecipato all'avventura: Stefano Calabrese, Aristide Fattori, Giampaolo Fresi Roglia, Luca Giancane, Davide Marrone, Lorenzo Martignoni, Luca Mayer, Antonio Nappa, Roberto Paleari, Emanuele Passerini.

Ecco il resoconto finale, scritto da Mattia.

I Guard@MyLAN0 (aka Chocolate Makers) dopo essersi qualificati terzi su 371 a maggio, grazie ai finanziamenti di Stephen Software, Microsoft Italia e ad un generoso contributo dell'Università degli Studi di Milano hanno partecipato anche alla finale: dall'8 al 10 agosto dieci studenti del nostro laboratorio http://security.dico.unimi.it sono stati a Las Vegas, Nevada.

Otto squadre in un grande salone, impegnate dieci ore al giorno per tre giorni, tentando di penetrare nei servizi preparati dagli organizzatori (i famosi Kenshoto) e attivi su tutte le macchine virtuali dei partecipanti. La gara si è rivelata molto impegnativa fin da subito, non appena ci siamo resi conto che chi giocava piu`vicino a casa era attrezzato assai meglio di noi, con potenti workstation e apparati per analizzare al meglio il traffico di rete. Anche la forza lavoro a disposizione era difformemente distribuita: alcune squadre avevano una trentina di persone di rincalzo che sostenevano lo sforzo comune dalle stanze vicine.

Dopo meno di mezz'ora i Shellphish (la squadra dell'Università di Santa Barbara, l'unica compagine con radici accademiche oltre alla nostra) erano gia` riusciti a compiere il primo attacco. Risultato notevole, se si tiene conto che praticamente tutti i servizi vulnerabili richiedevano l'analisi dei rispettivi binari x86 (FreeBSD). L'entusiasmo dei colleghi californiani è durato poco, però. In breve il sopravvento è stato preso da Sk3wl0fr00t, squadra capitanata da Chris Eagle, ben noto nell'ambiente per la sua familiarità con il debugger IDAPro. Ora dopo ora, il loro vantaggio è diventato davvero insormontabile e la lotta e` diventata per il resto del podio. Alla fine ci siamo piazzati solo quinti, ma con una grande soddisfazione. Infatti, grazie all'insonnia di alcuni dei nostri, siamo riusciti a risolvere il quiz proposto la sera del secondo giorno: "Shakespeare's longest nap". Un file contenente l'opera omnia di Shakespeare in formato ASCII doveva essere analizzato considerandone i byte come se fossero istruzioni x86, e identificandone la piu` lunga sequenza "che non contenesse accessi in memoria". Abbiamo così scoperto che Shakespeare, che già sapevamo essere stato un genio, ha introdotto una sfilza di più di 600 byte con queste caratteristiche.

La classifica finale è stata la seguente:

	Team	Steals	Overwrt	Brktrhu	SLA
1°	sk3wl0fr00t	1567	1046	9	69
2°	Routards	687	515	6	67
3°	1@stPlace	310	303	5	70
4°	Taekwon-V	521	276	5	68
5°	Guard@MyLAN0	347	138	2	60
6°	Shellphish	160	10	3	58
7°	Pandas with Gambas	55	81	8	70
8°	WOWHACKER	8	51	1	6

Gli Steals sono gli attacchi che hanno permesso di "leggere" un dato sulla macchina avversaria, gli Overwrites attacchi in cui si è "scritto", i Breakthrough sono punti assegnati per essere riusciti in un attacco prima di tutti gli altri e lo SLA indica la percentuale di tempo in cui i servizi sono stati attivi.

Se riusciremo ancora a partecipare sono sicuro che sapremo fare di meglio!

Per chi volesse approfondire i dettagli tecnici, rimando alleinformazioni raccolte da 1@stPlace http://nopsr.us/ctf2008/.

Autore: Mattia Monga

8. LA SICUREZZA DELLA RETE PER LA 44a PRESIDENZA USA

E' stato pubblicato il report finale della Commissione CSIS (Center for Strategic and International Studies) su **Cybersecurity for the 44th Presidency**: www.csis.org/component/option,com_csis_pubs/task,view/id,5157/type,1

A pagina 15, una considerazione sul presidente uscente ed un invito per Obama: "Let us be clear on the Bush administration's Comprehensive National Cybersecurity Initiative (CNCI): It is good, but not sufficient. The next administration should not start over; it should adopt the initial efforts of the initiative, but it should not consider it adeguate.

In diversi punti anche raccomandazioni per la messa in sicurezza degli Industrial Control System (ICS) e SCADA.

Autore: Enzo M. Tieghi

9. WPA: CAUTELA, NON ALLARMISMI

Recentemente si leggeva su alcuni siti che era emersa una falla nel WPA, sistema crittografico usato nelle reti wi-fi. Ho scritto qualcosa in proposito su uno dei miei blog e commentato su Zeus News e su Punto-Informatico questa notizia che riassumo anche qui brevemente.

Dei ricercatori tedeschi hanno sottolineato la possibilità in alcune stringenti ma verosimili condizioni che tramite attacchi del dizionario o chopchop modificato per il TKIP (il protocollo oggettivamente incriminato, non il wpa) si possono decifrare pacchetti corti come ARP e ARP response.

Questo è possibile in quanto il TKIP è stato progettato come soluzione legacy per quegli apparati aggiornabili che funzionavano solo con il WEP. Pertanto, di quest'ultimo si porta dietro alcune criticità (come il cipher RC4 e l'ICV (con MICHAEL e non con CRC32) ad ogni pacchetto cifrato.

Per il resto, nulla di nuovo sotto al sole se non un livello di attenzione che la problematica merita anche da parte dei non addetti ai lavori.

Al momento non mi risultano ancora disponibili paper della PacSec di Tokyo per leggere i dettagli dello studio presentato dai due ricercatori Erik Tews e Martin Becks (nella homepgae non particolarmente aggiornata campeggia un "Gone in

900 Seconds, Some Crypto Issues with WPA - Erik Tews", intervento di un'ora previsto a partire dalle 15.20 del 13 novembre scorso,ndr).

Nel frattempo, consiglio personale, se non potete disabilitare il TKIP e usare solo AES-CCMP, abbassate il rekeying time del TKIP a 60-120 secondi al massimo, per ora...

Autore: Armando Leotta

La versione pubblicata sul nostro blog http://blog.clusit.it/sicuramente/2008/12/wpa-cautela-non-allarmismi.html, contiene diversi link di approfondimento.

10. OFFERTA DI LAVORO

Società del settore telecomunicazioni, ricerca con urgenza su MILANO:

ESPERTI NETWORK SECURITY SU OS UNIX (rif. SEU/MI)

E' richiesta un'esperienza minima di 2-3 anni nell'ambito della sicurezza di reti e sistemi informatici su apparati Unix.

Sono richieste le seguenti competenze tecniche e professionali:

- Competenze in ambito sicurezza su sistemi UNIX Sun Solaris o UNIX HP;
- Ottime capacità di gestire le problematiche nelle modalità e nelle tempistiche definite;
- Autonomia operativa, puntualità e precisione;
- Buona conoscenza della lingua Inglese.

ESPERTI NETWORK SECURITY SU OS WINDOWS (rif. SEW/MI)

E' richiesta un'esperienza minima di 2-3 anni nell'ambito della sicurezza di reti e sistemi informatici su apparati Microsoft. Sono richieste le seguenti competenze tecniche e professionali:

- Competenze in ambito sicurezza su sistemi Windows;
- Ottime capacità di gestire le problematiche nelle modalità e nelle tempistiche definite;
- Autonomia operativa, puntualità e precisione;
- Buona conoscenza della lingua Inglese.

La tipologia contrattuale sarà in linea con le caratteristiche del candidato.

Chi fosse interessato può scrivere a info@clusit.it

11. NOTIZIE E SEGNALAZIONI DAI SOCI

La deadline per l'invio di eventuali segnalazioni dei soci per la pubblicazione sulla newsletter è il 25 di ogni mese

Rogue Security Softwares: che cosa sono e come evitarli.

Il socio Rossano Ferraris ci segnala che ENISA ha selezionato un suo articolo che tratta dei rogue security software, che in questi mesi stanno dilagando sulla rete Internet e costituiscono una vera e propria piaga se non si adottano le giuste raccomandazioni di prevenzione.

L'articolo, apparso sul magazine ENISA alle pagine 11-13, è intitolato: "A Threat Case Study: Rogue Security Software" ed è disponibile all'indirizzo

www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_12_08.pdf

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285

* associazione senza fini di lucro, costituita il 4 luglio 2000