Cyberfreedom – Pescara, 3 settembre 2005

INTERVENTO DI **STEFANO ZANERO**

Mi rendo conto che sono uno degli ostacoli tra voi e il pranzo, quindi ho deciso di eliminare le slides, ho deciso di eliminare buona parte del discorso, quindi tra poco mi alzo e me ne vado. Il problema di cui parlo un attimo impallidisce, perché stamattina ho sentito raccontare cose(e tutto sommato sono molto più percettibili e reali di quello di cui mi occupo io). E' molto più facile da un certo punto di vista capire la rilevanza di certi tipi di censura quando la rilevanza, nella mancanza di certi tipi di informazione. Io cerco di farvi capire la rilevanza della mancanza di altri tipi di informazione, un po più complessa. Buona parte della nostra è una frase fatta, buona parte della nostra vita di oggi viene gestita da, fatta con, comunicata tramite i calcolatori. Esistono fondalmentalmente due grandi industrie al giorno d'oggi i cui confini sono sempre meno distinguibili, è difficile distinguere chi fa videogiochi, chi fa intrattenimento, chi fa programmi per calcolatori. C'è la grande industria dell'ICT, è stata riunita infatti sotto un unico nome e c'è la grande industria del petrolio e della chimica, le due grandi industrie che in qualche modo condiscono la nostra vita. Nell'industria dell'ICT i componenti fondamentali, lo sappiamo tutti, sono due: l'hardware, le cose che si toccano, e il software, le cose che non si toccano, i programmi che fanno girare i calcolatori. All'interno dei programmi ci sono tutta una serie di istruzioni che dicono al calcolatore quello che deve e quello che non deve fare. E qui ci siamo arrivati, lo sappiamo tutti. Ora, se io, come diceva prima giustamente Carlo, come possiamo immaginare, se io sono una grossa casa automobilistica e mi metto a vendere un nuovo modello della mia casa automobilistica e vi dico, ve lo dico implicitamente, che questo modello è sicuro e poi una rivista del settore fa un test e detto modello di macchina si ribalta quando gira nel test, in generale succede che tutti quelli che hanno comprato la macchina si arrabbiano abbastanza, perché hanno pagato 20-25.000 euro per una cosa che rischia di ribaltarsi, e succede che la casa automobilistica, se non vuole fare la figura del cioccolataio, se non vuole fare la figura che ha fatto la FIAT con le Duna, decide che probabilmente prende le macchine e le fa sostituire a spese sue, rimettendoci un capitale pazzesco, e poi comincia a fare una pubblicità 'ah, questo tipo di macchina rimane incollata alla strada' la ricorderete sicuramente. Quando invece all'interno di un programma c'è una vulnerabilità di sicurezza succedono due cose: la prima, che è molto più facile far vedere le foto di una macchina che si ribalta piuttosto che le foto di un programma che crasha; la seconda, che non c'è una percezione mediatica, da parte dell'audience, anche solo da parte dei giornalisti che devono parlarne di cosa questo voglia dire. QUindi se io giornalista, come diceva prima giustamente qualcuno, è una vecchia massima del giornalismo, il giornalista è di base ignorante, si informa e traduce le cose che ha raccolto in modo da informare il prossimo. Questo dovrebbe essere il meccanismo grosso modo. Il meccanismo, l'abbiamo visto stamattina, è un po falsato. Quello che succede è che, se il giornalista non riesce a capire approfonditamentente qual è il problema e dove sono le dimensioni del problema, tantomeno riesce a comunicarlo a gente che ne sa meno di lui. Dov'è il problema? Il problema fondamentalmente è che il software che utilizziamo quasi tutti i giorni è scritto con i piedi, questo è un problema diffuso, lo sappiamo tutti, andiamo in banca 'vorrei l'estratto conto' 'eh, non glielo posso fare' 'perché?' 'eh, sa il computer' il computer non funziona. E' un classico, in banca succede, succede alle Poste, succede tipicamente verso le 11.30-mezzogiorno. Però questo è secondario. In generale sappiamo, abbiamo la percezione diretta per utilizzo proprio, che il computer si blocca di tanto in tanto. Ora, esisto degli errori all'interno dei programmi più o meno rilevanti. Sono dei problemi che portano semplicemente(semplicemente tra virgolette, perché se state viaggiando su un aereo un errore che porta semplicemente al blocco di un sistema informatico potrebbe non essere particolarmente gradevole) ma ci sono degli errori che portano semplicemente al fallimento del programma che state utilizzando. Chi usa Word per scrivere le lettere ne ha esperienza una ogni 15 minuti. Se però questi errori sono, affliggono fortemente i programmi(o programmi che hanno una rilevanza di sicurezza), ecco può succedere che sfruttando questi errori, mediante quello che viene chiamato exploit si può sfruttare una vulnerabilità che affligge un controllo di sicurezza, un programma, per ottenere un accesso che non dovremmo ottenere. Faccio un esempio così mi capite tutti tranquillamente. Sfruttando un

exploit in un sistema di banking online posso ottenere accesso al sistema di banking e, magari, al conto di qualcun'altro. E qui già parliamo, iniziamo a pensare, alla mistica figura dell'hacker approfittatore che abbiamo visto in tutti i film possibili e immaginabili. Non è quello perché qui stiamo parlando di cose più banali. Facciamo un esempio. Un noto gestore di telefonia, e già avete una scelta tra quattro, non vi dico quale, sull'UMTS, molto noto sull'UMTS, ha un portale, come tutti i gestori di telefonia da cui si possono comprare le ricariche, posso vedere lo stato del conto, attivare e disattivare tutti quei servizi che sembrano fantasticamente gratuiti e poi costano un mucchio di soldi ogni volta che li utilizzate. All'interno di questo portale una delle opzioni è vedere ciò che ho comprato negli ordini precedenti. Voi cliccate sull'ordine del vostro conto e vedete che si apre una stringa all'interno del vostro, nella barra degli indirizzi del vostro browser, del vostro programma che usate per navigare in rete, in cui c'è scritto a, una serie di caratteri strani, poi in fondo un punto interrogativo e poi dietro c'è scritto id= e un numero, che è il numero dell'ordine. Magari a voi non viene in mente, però ad altra gente viene in mente di provare a scrivere il numero prima e il numero dopo e vedere che cosa succede. Se quando scrivete il numero prima o il numero dopo vedete i conti di altre persone succedono due cose: uno, che chi ha progettato il sito è un emerito imbecille; due, che vi trovate con una patata bollente tra le mani, perché avete tre possibilità, ammesso di essere persone totalmente oneste ed integre avete tre possibilità: la prima, cliccare sull'iconcina che chiude il browser, far finta di niente e ' io non ho visto niente, non è successo' e state zitti, questo implica che da un lato non vi succede niente, dall'altro implica due piccoli problemi: il primo è che non vi potete grullare con gli amici, capisco che per l'essere umano medio possa non essere un problema ma qui non parliamo di esseri umani medi; il secondo problema, più grave, eticamente è che, io non ho fatto un esempio a caso, ho detto di una vulnerabilità che esiste ma è anche un esempio di una vulnerabilità che tutto sommato non è che porti proprio queste grandi traversie, un po di perdita di privacy, il fatto che la gente possa vedere nomi, cognomi ed indirizzi e i numeri di carta di credito del prossimo ma sono cose del tutto irrilevanti in fondo. Però in fondo di fronte a problemi più seri uno si crea il problema, ok io l'ho scoperto e non ci faccio niente, che succede quando lo scopre qualcun'altro? Se questo qualcun'altro è un altro pirla come me va bene così, non è successo niente. Ma se questo qualcun'altro è un malintenzionato, succede che c'è un sacco di gente potenzialmente, veramente un sacco di gente se pensate al sito di telefonia, che ci va di mezzo. E succede che in fondo è colpa mia, perché ho visto del fumo uscire da una casa e non ho chiamato i pompieri. E' la stessa cosa! Ho visto un ferito in mezzo alla strada, mi devo fermare a soccorrerlo, sennò mi incriminano per omissione di soccorso, giustamente tra l'altro. Se vedo una vulnerabilità di sicurezza in un sistema la devo raccontare, devo dire a qualcuno. E qui di nuovo ci sono le strade. Altra scelta: a chi lo racconto? Lo racconto pubblicamente o lo racconto privatamente a quelli che gestiscono questo sito? E quando lo racconto a questi che gestiscono questo sito come la prendono? La prendono del tipo 'ah, grazie! C'hai salvato la faccia!' o la prendo del tipo 'ah chiamiamo la polizia che abbiamo trovato un hacker'. Ultimamente la prendono nella seconda possibilità. Quindi tanta gente che trova questo vulnerabilità dice 'senti, facciamo che non l'ho vista, chiudiamo e basta'. Perché, come sempre, io non sono un politico, veramente mi sento all'esterno di questa cosa e vorrei fare un'osservazione: la legge e le procedure che forzano il rispetto della legge dovrebbero avere l'obiettivo di convincere le persone a tenere un comportamento migliore per la società. Se in una legge vi fossero una serie di applicazioni del tipo che convicono le persone a tenere un comportamento deteriore vuol dire che la legge, quella serie di applicazioni della legge, fanno acqua da qualche parte. E mi fermo qui perché io non sono la persona adatta a capire perché e come fanno acqua. Neanche a dire come migliorarla, io mi limito ad esporre un problema. E mi limito ad esporlo in altri termini. Succede che ci sia gente nel mondo abbastanza stupida, come il sottoscritto, da non fare nient'altro nella vita che pensare a come fare le cose in maniera più sicura, come fare in modo che non ci siano le vulnerabilità e magari passa anche la ditta perché è un altro altrettanto imbecille che decide di non andare negli Stati Uniti a prendere un posto di lavoro a 70mila dollari l'anno, ma di restare in una università a lavorare a 800 euro al mese, decide che la cosa più importante che può fare è cercare di insegnare le stesse cose a delle altre persone. Dopodiché si trova a gestire dei piccoli problemi del tipo 'ah, lo sa prof che ho sfondato il GPRS di X? Adesso cosa faccio?' 'Adesso che fai? adesso stai zitto! che vuoi che fai? Adesso cerchiamo il modo di informare X che hanno un problema senza che questi decidano che il loro problema sei tu'. E uno dice 'vabbé ma quanto sei

pavido? Cosa mai potrà essere successo?'. E allora vi racconto un'altra storia.
Quanti di voi lavorano in un ufficio? Alzate le mani per favore, fate finta di essere ancora svegli, ok? Quanti di voi adoperano le macchinette del caffé? Non le avete adoperate abbastanza perché vedo poche mani che si alzano. La macchinetta del caffé in ufficio ha un elemento dispositivo che è a chiavetta. Metto la chiavetta, metto il soldino, la macchinetta se è di un produttore particolarmente gentile mi fa pagare ben un centesimo in meno la bevanda e i soldi diventano dematerializzati e salvati sulla chiavetta. Ve la metto così. Questa chiavetta non è un dispositivo magico, è un dispositivo elettronico: da qualche parte le informazioni su come, su quanti soldi avete nella chiavetta stanno salvate. Ora, non è che ci voglia esattamente un genio per capire che se io prendo la suddetta chiavetta, la smonto, guardo che informazioni ci sono salvate sulla memorietta e le ricopio sopra uguale io avrò la chiavetta a lunga vita, cioè la chiavetta che ogni volta viene ricaricata in automatico. Non ci vuole un genio, lo capirebbe chiunque. Sta scritto a pagina 3 del libro di sicurezza che uso all'università. Ma è evidente, è banale, tant'è vero che il problema è stato già detto tante volte nella storia. E le carte dei telefoni a pagamento, e come fare a generare le ricariche dei cellulari in maniera che non si potesse adoperare una volta sola. Ci sono tante riproposizioni degli stessi problemi e ci sono tante soluzioni. C'è ne sono alcune che funzionano e c'è ne sono alcune che si sa non funzionano. Se tu, noto produttore di chiavette, scegli quella che non funziona, mi dispiace, ma hai scelto quella che non funziona. Allora che cosa succede? Succede che, bene o male, e daglie e daglie, e metti e metti l'euro, quando le chiavette entrano nelle Università dove si insegna come fare queste cose, di gente che prende la chiavetta e la smonta ne trovi. Di gente che dopo averla smontata spiega agli altri come fare ne trovi altrettanta. Il problema non è la gente che ha smontato la chiavetta, il problema è che tu produttore, prima di basare tutti i tuoi affari su un certo livello di chiavetta potevi porti il problema di come far si che questa chiavetta non potesse essere frodata. Non l'hai fatto, mi dispiace. Intendiamoci, non sono convinto che sia bene caricare le chiavette senza mettere gli euro, anzi è male. Ma non è male sapere come si fa. Ve l'ho spiegato in cinque minuti, lo avreste immaginato tutti come si fa avendo quel minimo di preparazione di elettronica di base. Chiunque lo può immaginare, questo non è un pensiero sbagliato, questo è il pensiero giusto, è quello che avrebbero dovuto avere altri che le hanno progettate le chiavette. Il pensiero sbagliato è 'ah quest'informazione è male che si sappia'. E allora mi riporta alla mente la famosa frase della moglie dell'arcivescovo di Canterbury, che di fronte alla scoperta di Charles Darwin che l'uomo discendeva dalle scimmie disse 'Oddio! Speriamo che non sia vero! O almeno speriamo che non si sappia in giro'. Diciamo che la voce è circolata un attimo, in alcune scuole americane non ancora ma arriveranno prima o poi. Il problema non è chi cambia il numero dell'applicazione, il problema non è chi scopre come si fa a bucare il sito, perché bucare il sito è una bella frase che viene adoperata a scopo di dare ad una parola una connotazione negativa. Il problema è che chi scopre come bucare un sito, bucare un programma, chi scopre la falla nel sistema di Microsoft, chi scrive il virus, chi scrive l'exploit, cioè il modo per sfruttare una falla, non ha fatto un'operazione cattiva, ha fatto un'operazione assolutamente naturale, ha preso in mano una roba e ha visto come si rompe. Se voi date in mano un giocattolo ad un bambino, la prima cosa che fa è smontarlo. Per questo i giocattoli migliori sono quelli fatti di un pezzo solo che poi combini con gli altri, i Lego. Perché il bambino li smonta, li rimonta, fa tutto quello che vuole ma quelli non si spaccano. Se voi gli date un giocattolo un po complicato 90% dei bambini lo spacca. Le persone che fanno il mio lavoro e quello di tanti altri in questa sala non sono mai cresciute, soffrono la sindrome di Peter Pan. E continuano a spaccare le cose, compresi gli attributi del prossimo. Il problema è che quanto spaccano troppo si trovano di fronte alle scelte che dicevamo prima: lo dico o non lo dico? Se non lo dico qualcun'altro lo scopre e magari questo qualcun'altro è più cattivo di me; se lo dico min fanno un mazzo così. La storia delle chiavette del caffé non l'ho tirata in ballo a caso, ma perché in questi giorni si sta continuando ad evolvere questa storia. Questo noto produttore di note macchinette per il caffé continua a cercare di far togliere, man mano che compare sulla rete qua e là il documento che spiega l'ovvietà che siccome sulle sue chiavette c'è memorizzata una cifra, se io ci scrivo sopra la stessa cifra ricarico la chiavetta. Non che questa cosa non si potesse fare in altro modo.
Allora ricapitolando il mio intervento, anche perché mi rendo conto che è il caso di arrivare ad una conclusione. Esistono degli oggetti che si chiamano programmi, nei programmi ci sono degli errori, gli errori li hanno messi i programmatori, coloro che li hanno fatti, involontariamente ma ce

li hanno messi. Questi errori restano lì dormienti finché qualcuno non li scopre. Questo qualcuno può essere un qualcuno buono o un qualcuno cattivo. Lasciamo stare quello cattivo. Abbiamo un qualcuno buono che scopre un errore, può fare due cose: o dirlo o non dirlo. Se non lo dice è l'equivalente dell'omissione di soccorso, non ha avvertito che c'era la probabilità che accadesse qualcosa di male. Andate sul sito delle 'Partners of security' degli Stati Uniti, c'è un bannerone enorme 'ah! vedi un'attività sospetta? segnalacela!'. Giusto. Allora se io vedo una cosa sospetta all'interno di un software la devo segnalare. A chi? Al produttore oppure al pubblico. Supponiamo per un momento di dare ascolto a chi dice 'la persona giusta a cui segnalarlo è il produttore'. Allora ci sono due tipi di produttore: quelli che possono non sapere, per esempio il produttore di un software, io ho trovato una vulnerabilità, lo informo perché potrebbe ragionevolmente non esserne a conoscenza perché è un errore. Hai fatto uno sbaglio. Quelli che non potevano non sapere, cioè se tu fai una chiavetta su cui puoi riscrivere la stessa cifra funziona ancora, non puoi non sapere che è un'idiozia. Questo è quello che diceva la moglie dell'arcivescovo di Canterbury è meglio non si sappia in giro, è il massimo che puoi fare. Ma prendiamo sempre il caso della buona fede. Allora segnalo questa cosa al produttore. Tipicamente quello che succedeva fino ad una decina di anni fa era: a, che molta gente non segnalava le cose ai produttori; b, che quando il produttore riceveva la segnalazione di una vulnerabilità la considerava alla stessa stregua di un qualunque errore nel software. Già molta gente ha scritto 'ah Word ogni 15 minuti mi mangia i file'. Vi pare che qualcuno abbia mosso un dito per fare qualcosa? La stessa cosa succedeva per le vulnerabilità. A meno che non fosse un qualcosa che in qualche modo era visibile, prossima versione del software forse si eliminava. Allora è cominciato il trend di quella che si chiama 'full disclosure', ovvero la pubblicazione, da parte di chi scopre le vulnerabilità, non solo del fatto che la vulnerabilità c'è ma anche di quale è la vulnerabilità. Cosa che ottiene tre risultati. Primo risultato. Spiega ad altri come è stata trovata la vulnerabilità. Che a volte può essere sempre la stessa storia, ci sono vulnerabilità, 'buffer overflow', che sappiamo da milioni di anni come si fanno, quali sono i problemi che portano a farli e ancora ci sono. Ma ci sono vulnerabilità che vengono scoperte, nuove, nuovi modi per bucare il software. E' importante che gli altri che fanno lo stesso lavoro lo sappiano. Io lavoro in un'università, faccio una ricerca, produco un'articolo scientifico, lo pubblico su una rivista internazionale. Perché? Perché è importante che gli altri sappiano quello che sto facendo io, perché sulla base di quello possono fare qualcos'altro. Quindi, primo motivo della 'full disclosure': pubblicazione scientifica. Secondo motivo della 'full disclosure': allerti le persone. Mi si ribalta la macchina durante un test, lo dico alla casa produttrice. La casa produttrice mi dice 'opp! che spendo tutti i milioni di euro che servono per rifare la macchina e ridarla a tutte le persone che già l'han comprata? cosa faccio?' Ma vado su un giornale, sparo a zero su questa casa responsabile che sta facendo una cosa irresponsabile. Dò pubblicità alla cosa, ok? Grido: 'Al lupo! Al lupo!'. Quindi dare pubblicità serve nel caso in cui si riscontra una certa immobilità del vendor a dare l'allarme alle persone, a dire 'guardate che quest'applicazione non è sicura'. Terzo scopo, che è correlato al precedente: siccome il vendor se gli dici 'guarda, ho trovato una vulnerabilità' magari tra 6, 12 mesi la chiude. Gli dico 'guarda ho trovato la vulnerabilità. se ti serve del tempo per chiuderla fammelo sapere. Sennò presumo che non sei interessato quindi tra due settimane io la pubblico'. E tipicamente questo ha il risultato di farti ricontattare dalle persone che stanno cercando di risolvere il problema oppure che fingono di starci accanto. Quindi la 'full disclosure' è servita a tre cose: a, rendere più accellerato il meccanismo di scoperta di come si rompe un software, è il processo scientifico, più si pubblica, più gente sa le cose, più può costruire delle altre cose sulla base di queste; seconda cosa, si rende edotto il pubblico(fino a 10-15 anni fa anche amministratori di sistema mediamente competenti magari non sapevano niente del fatto che il loro sistema Unix preferito era pieno di buchi o che il loro sistema Windows preferito era pieno di buchi. Adesso chiunque, almeno a livello superficiale, lo sa che un sistema esposto in rete è un sistema vulnerabile e ci sono una serie di mantra che sono entrati nell'anticamera del cervello delle persone che si occupano di informatica); terzo effetto, i vendor sono dovuti passare da una politica del tipo 'si vabbé lo fixo tra due anni quando faccio la nuova release del prodotto' a 'forse è meglio che lo fixo fra tre giorni prima che qualcun'altro lo scopra e crei un bel worm che si propaga sfruttando questa stessa vulnerabilità'. Problema: siccome a nessuno piace fare la figura del fesso, tanto meno se ha speso milioni e milioni di euro in pubblicità che dicono '*, nome del produttore ambregalo' e poi scopri che il giorno dopo che inizia ad uscire questa campagna la gente inizia a far piovere

vulnerabilità su vulnerabilità su vulnerabilità su questo povero prodotto, siccome questa cosa non sta simpatica a nessuno, diciamocelo, anche quando si correggevano i compiti alle superiori ci stava un po' sulle balle il professore che correggeva i compiti, si ho sbagliato, ma non c'è bisogno che tu mi fai tutto il circoletto rosso e mi togli il punto, insomma. Siccome il circoletto rosso dà fastidio, chiaro che un vendor, una casa produttrice cerca il più possibile di far star zitto questi grilli parlanti che raccontano queste cose che non andrebbero raccontate. Come si fa a farli star zitti? In tutti i modi. Li paghi, ma questo è escluso perché se i grilli parlanti diventano troppi e costano troppo inizia a diventare pesante la cosa. Oppure li screditi perché li chiami hacker. Ormai è il nome che si sono dati loro, è fatto diventare un nome negativo e usi quel nome per etichettarli. Ma anche questa scricchiola dopo un po', alla lunga diventa difficile dire 'ah si si' dopo un po' si spera che la gente si svegli. C'è un terzo modo: fargli causa. Allora, fermo restando che viviamo in un fantastico stato di diritto e quindi il bene trionfa sempre, il male viene sconfitto, arrivano i cavalieri e uccidono il drago, nel momento in cui, e lo diceva qualcuno oggi, ed è un'analogia abbastanza interessante, non serve che io abbia torto per far si che la minaccia di farmi causa mi faccia stare zitto. E' il semplice fatto di farmi causa che basta a farmi stare zitto, è la semplice prospettiva. Perché? Perché se io sono IBM e Microsoft mi fa causa per una cosa che riguarda il mio business IBM mettiamo sul tavolo soldi e avvocati come se piovesse e vediamo chi vince. Perché ho i soldi per farlo. Ma se io sono PincoPallino e scopro la vulnerabilità del programma di telefonia e il portale di telefonia minaccia di farmi causa, a me che sono PincoPallino ma chi me lo fa fare di andare a rompergli le scatole? ma cosa ci guadagno? niente. Cosa rischio di perderci? Tanto. E allora sto zitto. E questo meccanismo un po' perverso sta lentamente avendo la meglio sulla 'full disclosure'. Allora, concludendo, non è una cosa altrettanto percettibili di quelle che abbiamo visto stamattina. E' una cosa su cui c'è tanta informazione, nel senso di materiale reperibile su Internet(nel senso che se cercate 'full disclosure debate' su Google trovate di tutto). Il punto chiave è, e ve lo chiedo(ma fatemi sapere la vostra idea): la colpa, o meglio il cerino che in questo momento sta acceso e pericolosamente vicino alle dita delle mani dei ricercatori che trovano le vulnerabilità, è giusto che sia lì? E' colpa loro? L'insicurezza delle reti è colpa di chi rilascia gli exploit nella 'full disclosure' o è colpa di chi ha messo le vulnerabilità nel software per incapacità, inettidudine, chiamatela come volete? E, se la colpa non è di chi scopre il problema, ma di chi il problema l'ha fatto, come facciamo a prendere questo circo mediatico, a scaricare la colpa sempre sulle stesse persone e rigirarle in maniera tale che, come è successo all'industria automobilistica con il requisito di sicurezza, come è successo per le linee aeree e il rischio di sicurezza già sappiamo come è andato a finire e come è successo con tante altre industrie in cui delle 'regulation' alla fine hanno fatto in modo che alla fine si passasse dal 'è sempre colpa di qualcun'altro' al 'beh è colpa mia che gli aerei, le macchine o qualcos'altro lo faccio, se l'aereo, la macchina esplode'. Allora forse è il caso di rifletterci perché non è mai colpa di chi questo software lo fa, lo vende e, se permettete un pizzico di invidia, ci guadagna anche un sacco di soldi sopra. E io con questo ho finito di annoiarvi.