

CRYPTO-GRAM  
15 luglio 2004

Scritta da Bruce Schneier  
Fondatore e CTO di Counterpane Internet Security, Inc.

Edizione italiana curata da Communication Valley SpA

E-mail: [schneier@counterpane.com](mailto:schneier@counterpane.com)

Web: <<http://www.schneier.com>> oppure <<http://www.counterpane.com>>

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

Crypto- Gram in versione originale è anche consultabile in formato RSS:  
<<http://www.schneier.com/crypto-gram-rss.xml>>

\*\* \*\*

In questo numero:

Il giusto processo e la sicurezza

Note di sicurezza da ogni dove: Le macchine a raggi X e la sicurezza negli edifici

I crittografi e l'Ufficio Immigrazione statunitense

Le ristampe di Crypto- Gram

La sicurezza e i dispositivi di archiviazione portatili

News

Le News di Counterpane

Note di sicurezza da ogni dove: La Coca-Cola e la NSA

Il Canile: ICS

Il CLEAR Act non contribuisce a contrastare il terrorismo

Commenti dei lettori

\*\* \*\*

Il giusto processo e la sicurezza

La Corte Suprema degli Stati Uniti si è recentemente pronunciata sui tre ricorsi legati alle manovre legali contro il terrorismo messe in atto dall'amministrazione Bush. Questi casi sono stati infinitamente discussi nell'ambito delle libertà legali e civili e si è deciso, in larga misura ma non completamente, a favore della presunzione di innocenza e del giusto processo.

Ma intendo parlare di quanto siano importanti tali decisioni per la sicurezza della nazione. La sicurezza ha moltissime sfaccettature; esistono numerose minacce provenienti da direzioni altrettanto numerose. Il concetto di sicurezza comprende la sicurezza delle persone nei confronti del terrorismo, ed anche la sicurezza delle persone nei riguardi di un governo di tipo tirannico.

I tre ricorsi sono tutti simili fra loro, con lievi variazioni. In un caso, le famiglie di 12 kuwaitiani e di due australiani imprigionati a Guantanamo Bay sostengono che la loro detenzione è illegale secondo quanto stabilisce la legge statunitense. Negli altri due casi, gli avvocati domandano se sia lecito che due cittadini statunitensi -- uno catturato negli Stati Uniti, l'altro in Afghanistan -- possano essere trattenuti indefinitamente senza accuse formali, senza un processo, senza che possano far ricorso ad un legale. In tutti questi casi, l'amministrazione sostiene che tali detenzioni rientrano nella legge, essendo basate sull'attuale "guerra al terrorismo". I querelanti affermano che queste persone possiedono dei diritti garantiti dalla Costituzione americana, diritti che non possono essere cancellati.









posso già evitare lunghe code in moltissimi aeroporti sfruttando delle corsie speciali. I passeggeri di prima classe hanno gli stessi privilegi. Ma quali altre persone potrebbero usare un sistema come questo? Non riesco a capirne il target.

< [http://www.boston.com/business/articles/2004/06/28/minn\\_airport\\_starts\\_advance\\_security\\_check\\_s](http://www.boston.com/business/articles/2004/06/28/minn_airport_starts_advance_security_check_s)> oppure < <http://tinyurl.com/5z48t>>  
< <http://www.cnn.com/2004/US/Midwest/06/28/airport.background.checks.ap/index.html>> oppure  
< <http://tinyurl.com/2v8gu>>  
< <http://www.startribune.com/stories/1631/4847379.html>>  
< <http://www.startribune.com/stories/1576/4864503.html>>

Analisi del Manoscritto Voynich:

< <http://www.sciam.com/article.cfm?chanID=sa006&colID=1&articleID=0000E3AA-70E1-10CF-AD1983414B7F0000>> oppure < <http://tinyurl.com/2xung>>

Un diffuso programma di backdoor ha una backdoor al suo interno.

< <http://www.securityfocus.com/news/8893>>

Evitare il furto di identità: un piccolo vademecum.

< <http://www.securityfocus.com/news/8908>>

La tortura ha avuto un ruolo di primo piano nelle notizie, sin dall'11 settembre 2001, e recentemente in merito alle pratiche dell'esercito statunitense nel carcere di Abu Ghraib in Iraq. La politica non è un campo di mia competenza, e non ho intenzione di discutere sugli aspetti politici dello scandalo. Non intendo nemmeno dibatterne le questioni morali: è morale torturare un dinamitardo per scoprire un ordigno nascosto e pronto ad esplodere, è morale torturare un innocente affinché qualcuno disinnesci l'ordigno, oppure è morale torturare N-1 persone per salvare N vite? Ciò che più mi interessa sono le implicazioni di sicurezza legate alla tortura: quanto funziona come contromisura di sicurezza, e quali sono i compromessi, cosa si ottiene in cambio? Quelli che seguono sono due studi eccellenti che dimostrano quanto inefficace sia la tortura. Dato che essa non produce in effetti nessun tipo di utili informazioni di intelligence, perché diamine stiamo spendendo così tante energie nel mondo per portarla avanti?

< [http://www.salon.com/opinion/feature/2004/06/18/torture\\_1/index.html](http://www.salon.com/opinion/feature/2004/06/18/torture_1/index.html)>  
oppure < <http://tinyurl.com/57668>>  
< [http://www.salon.com/opinion/feature/2004/06/21/torture\\_algiers/index.html](http://www.salon.com/opinion/feature/2004/06/21/torture_algiers/index.html)>  
oppure < <http://tinyurl.com/4v29z>>

Ottimo discorso di Cory Doctorow sul digital rights management:

< <http://craphound.com/msftdrm.txt>>

È ancora molto semplice ingannare i rilevatori di impronte digitali:

< <http://www.ep.liu.se/exjobb/isy/2004/3557/>>

Un buon articolo sulla programmazione approssimativa e la sicurezza:

< <http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=160>>

Il CERT avverte di non utilizzare Internet Explorer (io sono un felice utente di Opera).

< [http://www.theregister.co.uk/2004/06/28/cert\\_ditch\\_explorer/](http://www.theregister.co.uk/2004/06/28/cert_ditch_explorer/)>

Ottimo articolo sulle origini di uno scherzo diffuso in Internet: quello secondo cui Bill Gates starebbe pagando per tener traccia delle vostre email.

< <http://www.wired.com/wired/archive/12.07/hoax.html>>

Sette buone abitudini di aziende estremamente sicure:

< <http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=56003>>

Lasciamo stare le varie questioni. Chi ha il sito Web più sicuro: Bush o Kerry?

< <http://www.wired.com/news/infostructure/0,1377,64036,00.html>>

La sicurezza di un aeroporto ha introdotto dei veri esplosivi in un bagaglio per mettere alla prova alcuni cani anti-bomba. Problema numero uno: hanno perso le tracce di quel bagaglio. Problema numero due: si trattava di un vero bagaglio appartenente a un ignaro passeggero.

< [http://www.alibi.com/editorial/section\\_display.php?di=2004-05-20&scn=news#8167](http://www.alibi.com/editorial/section_display.php?di=2004-05-20&scn=news#8167) >

oppure < <http://tinyurl.com/6g4as> >

La tabella di marcia per sistemare una falla di sicurezza di Mozilla. È impressionante la rapidità e la competenza con cui è stata gestita.

< <http://www.sacarny.com/blog/index.php?p=104> >

Fare hacking per guadagnare:

< <http://www.computerworld.com/securitytopics/security/story/0,10801,94407,00.html?nas=SEC-94407> > oppure < <http://tinyurl.com/4k46u> >

La Guida dell'FBI sulle armi occultabili:

< <http://datacenter.ap.org/wdc/fbiweapons.pdf> >

Rapporto sulla sicurezza delle reti DOD canadesi:

< <http://www.canada.com/national/nationalpost/news/story.html?id=d47120ad-92eb-40d0-a9c3-f47216966493> > oppure < <http://tinyurl.com/6uhlm> >

Ecco un bell'atteggiamento nei confronti della sicurezza. L'articolo tratta di un buco di Friendster che permette agli utenti di ottenere informazioni su chi sta guardando i loro profili online. "Una volta informata dei buchi di sicurezza che Moore e Chisholm hanno exploitato, la rappresentante di Friendster Lisa Kopp insiste, 'Abbiamo una linea di condotta tale per cui non siamo sotto hacking'. Quando ho spiegato che, condotta o non condotta, Friendster è sotto hacking, ha risposto: 'La sicurezza non è una priorità per noi. Noi siamo maggiormente concentrati sul rendere il sito sempre più veloce'".

< [http://www.wired.com/wired/archive/12.06/dating\\_pr.html](http://www.wired.com/wired/archive/12.06/dating_pr.html) >

\*\* \*\*

Le news di Counterpane

Counterpane ha un nuovo libro bianco su come il monitoraggio contribuisca alla conformità. Dato che sempre più aziende non riescono a rientrare nei criteri di Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, ecc., la conformità sarà un aspetto ancora più importante per la sicurezza.

< <http://www.counterpane.com/compliance.html> >

Abbiamo un altro documento sulla nostra Enterprise Protection Suite, il nostro pacchetto integrato di servizi per la sicurezza. Incentrato sul monitoraggio, con EPS le aziende possono rendere le proprie reti sicure, e velocemente.

< <http://www.counterpane.com/overview.html> >

\*\* \*\*

Note di sicurezza da ogni dove: la Coca-Cola e la NSA

La Coca-Cola lancia un nuovo concorso. Nascosti all'interno di 100 lattine di Coca vi sono una SIM card, un trasmettitore GPS, e un microfono. I vincitori attivano la lattina premendo un pulsante, ed essa effettuerà una chiamata a una centrale di monitoraggio. Dopodiché i vincitori verranno individuati grazie al trasmettitore GPS e il loro premio sarà consegnato a sorpresa.

Gli ingegneri della NSA bevono Coca-Cola. Molta Coca-Cola. La possibilità che un microfono attivo all'interno di una lattina di Coca penetri in una delle infrastrutture ad alta sicurezza della NSA è da tenere in considerazione. Un'analisi ragionevole della minaccia potrebbe essere di questo tipo: "Vedete, le probabilità che una di queste 100 lattine, su centinaia di milioni di lattine prodotte, finisca nelle nostre strutture sono estremamente basse -- diciamo una su centomila -- per cui non val la pena preoccuparsi".

Ma l'Information Staff Security Office, l'ufficio per la sicurezza della NSA ha stabilito diversamente: "È importante che TUTTE le lattine di Coca-Cola all'interno dei nostri spazi siano ispezionate. Questo comprende le lattine già all'interno dei nostri edifici e quelle che vengono distribuite quotidianamente. Se scoprite una delle lattine speciali, NON attivatela. Invece, allertate subito l'ISSO e riferite l'incidente".

Tutto questo è pura isteria. Ma vi immaginate ispezionare ogni lattina di Coca che entra alla NSA, aprire ognuna delle centinaia di confezioni di Coca e verificare se c'è un trasmettitore GPS? Quanto verrà a costare tutto ciò? Che cosa NON starà facendo la NSA perché sarà impegnata in questo inutile lavoro?

Naturalmente gli ingegneri alla NSA stanno già creando lattine di Coca con le antenne, circuiti integrati e tastierini, per poi lasciarle vicino ai distributori di snack come scherzo.

E dov'è la Pepsi in tutto questo? Non dovrebbero reclamizzare la loro "coca senza sorveglianza"?

La faccenda suona divertente, ma c'è anche un aspetto molto serio. Ancora una volta le decisioni sulla sicurezza sono offuscate da ben altre priorità. La linea di condotta della NSA sull'ispezione delle lattine di Coca è un chiaro esempio di salvaguardia dei propri interessi. Qualche dirigente all'interno della NSA non ha voluto rispondere personalmente di un eventuale ricevitore GPS introdotto superando la sicurezza, e allora ha deciso che ogni cosa deve venire ispezionata. Per il grande pubblico è un rischio assai minimo, ma non è così per lui. Le sue priorità sono ben diverse da quelle della società, ma dato che a lui importano di più le sue priorità, ed è una sua decisione, ecco tutto quel che ne consegue.

Noi, come società, dobbiamo capire come affrontare i compromessi e i bilanciamenti di sicurezza in un altro modo. Il fatto che siano certi individui o certe grandi aziende a realizzare compromessi e bilanciamenti di sicurezza per noi basandosi sulle \*loro\* priorità non ci rende certo più sicuri, e ci sta costando parecchio denaro.

< <http://www.wired.com/news/technology/0,1282,64078,00.html> >

\*\* \*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

Il Canile: ICS

ICS di Atlanta ha sviluppato l'algoritmo crittografico "Tree".

In che cosa Tree è diverso? Beh, anzitutto "non utilizza alcuna matematica". Non sono molto sicuro di come ciò sia possibile su un computer, ma questo è quanto dichiara il creatore di Tree. Da uno scambio di email: "...Il 99,99% delle persone utilizza la matematica per codificare e poi per 'rompere' il codice. Dato che noi non la utilizziamo davvero, sarà molto difficile decodificare il codice".

Non solo non fanno uso di matematica, ma non hanno una chiave. "Tree non utilizza una 'chiave'... Mi basta inserire il testo, premere 'Codifica' e puf, ecco il messaggio cifrato. Per la decodifica, inserisco i messaggi cifrati, premo 'Decodifica' e puf, ecco fatto. Tutto qui. Niente chiave".

Impressionante.



diventare ufficiali dell'immigrazione significa meno forza lavoro per investigare altri reati, e questo rende tutti noi meno sicuri.

I terroristi rappresentano solo una piccolissima minoranza di qualsiasi cultura. Una delle cose più importanti che una buona forza di polizia mette in atto è quella di mantenere buoni contatti con la comunità locale. Se, ad esempio, voi sapeste che ogni volta che contattate la polizia i vostri registri venissero controllati alla ricerca di multe non pagate per divieti di sosta, per libri non restituiti alla biblioteca e altre violazioni non penali, in che luce vedreste i poliziotti? È molto più importante che le persone si sentano sicure e senza timori quando contattano le forze dell'ordine.

Quando un immigrato musulmano nota qualcosa di sospetto nell'appartamento accanto, vogliamo che lui chiami la polizia. Non vogliamo che abbia il timore che la polizia possa deportare lui e la sua famiglia. Non vogliamo che lui si nasconda se la polizia arriva e comincia a far domande. Vogliamo lui e la comunità dalla nostra parte.

Trasformando agenti di polizia in ufficiali dell'immigrazione, il CLEAR Act e il HSEA non faranno altro che dissuadere il prossimo Danny Sigi dal riferire reati o attività sospette. Questo danneggerà la sicurezza nazionale molto di più di qualsiasi beneficio derivato dall'individuazione di violazioni di immigrazione non penali. Si aggiungano i costi derivati dall'aver poliziotti a caccia di irregolarità d'immigrazione invece di rispondere a crimini veri e propri, e si otterrà uno dei peggiori compromessi di sicurezza.

Questo articolo è stato originariamente pubblicato su CNet:

< <http://news.com.com/CLEARly+muddying+the+fight+against+terror/2010-7348-3-5236260.html> > oppure < <http://tinyurl.com/2yb9x> >

\*\* \*\* \* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\* \*\*\*\*\*

## Commenti dei lettori

Da: Anonimo

Oggetto: Witty

Lei ha scritto: "Witty è stato scritto molto rapidamente. La compagnia di sicurezza eEye ha scoperto la vulnerabilità nei prodotti di ISS, BlackICE e RealSecure, l'8 marzo, e ISS ha rilasciato una versione con patch il 9 marzo. eEye ha pubblicato una descrizione molto accurata e tecnica della vulnerabilità il 18 marzo. La sera del 19 marzo, circa 36 ore dopo la divulgazione pubblica da parte di eEye, il worm Witty veniva lasciato libero di agire."

Abbiamo eseguito l'aggiornamento del nostro BlackIce il 17 marzo (mercoledì) e in seguito abbiamo controllato, con la versione aggiornata, che non vi fossero altri update disponibili (sempre mercoledì). Il 20 marzo (sabato) Witty è comparso e il computer in questione è stato distrutto.

Per me la cosa più notevole di tutta questa vicenda è l'atteggiamento mostrato da ISS per dare ad intendere che non si trattasse di un grande problema. La patch disponibile una settimana prima -- ma andiamo! (e confermo di avere un valido contratto di supporto). Avrei preferito un maggior impegno nel comunicare la riparazione alla gente, invece di correggere la storia in un secondo momento; purtroppo quest'ultima cosa è forse più redditizia con i clienti nuovi e con chi non è stato affetto dal problema, mentre gli altri clienti sono magari già considerati "persi".

Mi ci è voluta mezza giornata per ripristinare il computer, e qualcosa è andato perduto, ma niente di estremamente importante. Questo trend di virus distruttivi mi preoccupa più per gli utenti domestici, che conservano molte cose "preziose" sulle loro macchine, come ad esempio foto digitali di momenti importanti, e nessun backup. Distruggere questo genere di dati è un crimine davvero disgustoso,

secondo il mio modo di vedere (in più, in un mondo in cui i computer sono sempre più considerati degli elettrodomestici, il numero di opportunità per arrecare simili danni non potrà che aumentare).

Spero che Witty possa servire a migliorare le cose, dimostrando ai rivenditori di prodotti per la "protezione" come le falle in essi presenti siano particolarmente critiche, e dimostrando che, se non si comportano in maniera esemplare, le conseguenze ricadranno sul loro portafoglio, perdendo clienti che non rivedranno. Penso che questo sia l'unico processo in grado di essere d'aiuto con i prossimi virus come Witty. Sfortunatamente, come accade in politica, presumo che molte aziende continueranno a pensare che sia più economico investire in pubbliche relazioni dopo l'evento, invece che prevenire i danni. Speriamo di avere torto.

Da: Mart van de Wege <[mvdwege@myrealbox.com](mailto:mvdwege@myrealbox.com)>  
Oggetto: Codici usa- e-getta per il banking elettronico

Nella sua Crypto-Gram di giugno, ho notato questo passaggio: "Per una maggior sicurezza, lei poi estrae una scheda che contiene 50 codici usa e getta. Jubran usa i codici, uno dopo l'altro, ogni volta che effettua un login o una transazione. La sua banca, la Nordea PLC, le invia automaticamente una nuova scheda poco prima che la precedente sia esaurita".

Ho l'impressione che Wired non sia molto aggiornato a riguardo. Questo sistema è in uso da parecchi anni nella banca olandese Postbank.

Il suo sistema Girotel funziona innanzitutto richiedendo un login dell'utente con un cosiddetto GIN (Gebruikers Identificatie Nummer, ovvero Numero di Identificazione Utente). Dopodiché, Girotel impone la conferma di ogni transazione mediante un TAN (Transaction Authentication Number, cioè Numero di Autenticazione Transazione). Questi codici TAN vengono forniti al cliente sotto forma di elenco cartaceo, e ne vengono aggiunti di nuovi quando il cliente si ritrova con un numero limitato di TAN (credo la soglia sia 10, ma non ne sono certo).

Questo sistema è in funzione da almeno dieci anni a questa parte, con grande soddisfazione sia della banca che degli utenti. La sua caratteristica di non essere legato ad alcuna piattaforma ha permesso a Postbank di aggiornare il software da un client stand-alone che si connette telefonicamente a una versione online, senza cambiare interfaccia e senza compromettere la sicurezza.

Da: "Bryan L. Fordham" <[bfordham@socialistsushi.com](mailto:bfordham@socialistsushi.com)>  
Oggetto: Documenti d'identità nazionale

I lettori europei le hanno scritto "Ho avuto la mia carta d'identità nazionale per X anni e ho dovuto mostrarla alla polizia solo una volta. Per il resto la uso per votare, comprare alcolici, ecc."

Ciò sembra rafforzare la posizione contraria a questi documenti, e non indebolirla. Se li si è mostrati solo una volta, non sembrano essere molto utili; e come possono contribuire alla sicurezza? E in secondo luogo, la mia patente di guida già mi permette di dimostrare chi sono e quanti anni ho quando vado a votare. Perché dovremmo avere un altro documento?

Da: "Steven Shaer" <[steve@shaer.com](mailto:steve@shaer.com)>  
Oggetto: I codici iraniani, eccetera...

Per quanto concerne il suo articolo sulla decodifica dei codici iraniani, a mio parere lei ha ignorato un altro scenario altrettanto ovvio: forse la CIA/NSA hanno comunicato di proposito a Chalabi che avevano decodificato i codici iraniani, e forse lo hanno fatto proprio perché non avevano decodificato i codici. Uno può immaginare svariate situazioni in cui si vorrebbe che il proprio avversario CREDESSE di aver decodificato i nostri codici, quando così non è. Compreso il fatto che gli Stati Uniti volevano che l'Iran cambiasse la propria tecnologia (per la quale gli USA non avevano una back-door) passando a

una tecnologia per la quale gli USA avevano una back-door. Un'altra possibile ragione potrebbe essere il creare sospetti all'interno del governo iraniano su certi individui che potrebbero essere utili per gli interessi statunitensi.

Da: Toby Bryans <[toby@bryans.org](mailto:toby@bryans.org)>

Oggetto: Re: Il jamming dei telefoni cellulari e gli attacchi terroristici

Tutta questa vicenda è particolarmente fastidiosa, dato che l'unica funzionalità dei telefoni cellulari usati durante gli attacchi è stata la sveglia. Non sono stati chiamati per detonare -- avevano tutti una sveglia regolata su un certo orario. Non è nemmeno necessario che siano accesi, visto che alcuni modelli di cellulari possono attivarsi da soli se è impostato un allarme.

Bloccare i cellulari non farà nessuna differenza per questo attacco. Già che ci siamo, perché non vietare alla gente di portare orologi da polso?...

Naturalmente, vi sono esempi di opportunismo politico da entrambe le parti:

<[http://news.bbc.co.uk/1/hi/uk\\_politics/3602019.stm](http://news.bbc.co.uk/1/hi/uk_politics/3602019.stm)>

...che comunque non farebbero alcuna differenza per questo attacco in particolare.

Da: Alexey Kirpichnikov <[alexkir@r66.ru](mailto:alexkir@r66.ru)>

Oggetto: Fare fotografie in metropolitana e gli attacchi terroristici

Vivo a Ekaterinburg, in Russia, e vorrei dire che è tuttora vietato fare fotografie nella nostra metropolitana. Non ne conosco le ragioni e la cosa mi sembra piuttosto strana. :) Penso che anche gli ufficiali di sicurezza qui si siano resi conto che questo divieto non ha alcun senso, perché i miei amici hanno provato a fare fotografie in metropolitana e sono stati ignorati dai poliziotti.

Eppure, cartelli "vietati foto e video" si trovano dappertutto nelle stazioni della metropolitana.

\*\* \*\*

CRYPTO-GRAM è una newsletter mensile gratuita che offre riassunti, analisi, approfondimenti, e commenti sulla sicurezza (informatica e in generale) e sulla crittografia.

La versione italiana è curata da Communication Valley SpA <http://www.communicationvalley.it/>.

Per iscriversi o cancellarsi andare all'indirizzo <http://www.cryptogram.it/>.

I numeri arretrati sono disponibili all'indirizzo <http://www.cryptogram.it/>.

Per informazioni [crypto-gram@communicationvalley.it](mailto:crypto-gram@communicationvalley.it).

Inoltrate liberamente CRYPTO-GRAM a colleghi ed amici che possano trovare questa pubblicazione di un certo interesse. Viene concessa l'autorizzazione a ristampare CRYPTO-GRAM, a condizione che sia stampata integralmente.

CRYPTO-GRAM è realizzata da Bruce Schneier. Schneier è l'autore dei best seller "Beyond Fear", "Secrets and Lies" [tradotto in Italia col titolo "Sicurezza Digitale"] e "Applied Cryptography", e inventore degli algoritmi Blowfish, Twofish e Yarrow. È il fondatore e CTO di Counterpane Internet Security, Inc., e membro del comitato consultivo dell'Electronic Privacy Information Center (EPIC). Scrive spesso e tiene conferenze in merito alla sicurezza informatica e alla crittografia. Il suo sito Web è all'indirizzo <<http://www.schneier.com>>.

Counterpane Internet Security, Inc. è leader mondiale nel monitoraggio guidato della sicurezza informatica. Gli analisti esperti in sicurezza di Counterpane proteggono reti per aziende inserite nella Fortune 1000 a livello mondiale.

Copyright (c) 2004 by Bruce Schneier.