BARATA ELETRICA, numero 3
Sao Paulo, 15 de abril de 1995

Conteudo:

Creditos:

Este jornal foi escrito por Derneval R. R. da Cunha
Com as devidas excecoes, toda a redacao e' minha. Esta' liberada a copia (obvio) em formato eletronico, mas se trechos forem usados em outras publicacoes, por favor incluam de onde tiraram e quem escreveu. Aqueles interessados em receber futuras edicoes deste ou de outro jornal (nao sei se ira' continuar com esse titulo) mandem um mail eletronico para:
wu100@fim.uni-erlangen.de

INTRODUCAO:

Entramos no mes de abril, Pascoa. Nao foi dessa vez que a reuniao que a reuniao que eu planejava aconteceu. Problemas pessoais e de ordem financeira me impediram de planejar a coisa. Traduzindo: faltou tempo e grana. Minha renovacao de bolsa foi postergada e a vida nao ta' facil. O envio da ultima edicao do Barata Eletrica tambem me custou um pouco de imaginacao. Como nao podia usar os computadores da USP para fazer o envio, usei uma conta que eu tenho na Europa. Chique, porem necessario. Quando voce tem acesso via telnet, e' muito dificil barrar seu acesso a uma conta Internet legitima da qual voce pode pelo menos manter contato com pessoas.

O grande problema e' que no acesso telnet, existe uma diferenca de tempo muito grande entre aquilo que voce tecla e o que aparece na tela. Para fazer acontecer a coisa, eu tive que descobrir uma caracteristica de todo mail decente, que e' a possibilidade de fazer uma lista de correspondencia ou "alias". Da primeira vez, eu pensei em fazer uma coisa meio ilegal, que e' o "fake mail". Para quem nao sabe, fake-mail e' uma forma de se enviar um "e-mail" com endereco de remetente falso. E' complicado (para quem nao sabe), e de qualquer forma, pode-se rotear (no sentido de descobrir a rota) o envio do dito, de forma que, se a carta foi enviada de computador tal, basta uma chegada nos arquivos para se saber de onde e' que alguem fez o tal envio.

Muita gente usa esse recurso para enviar cartas anonimas ou de gente famosa, como o presidente dos EUA. Um "inteligente" la' nos EUA resolveu usar esse recurso para enviar uma carta de ameaca ao presidente. Nao vou dizer que ele nao foi esperto. Acontece que isso e' um crime serio naquelas bandas, e o Servico Secreto checa qualquer carta, por mais idiota que seja. Descobriram o computador de onde foi enviado e tambem que o cara que fez a coisa nem tinha conta naquele servidor Internet. Foi processado nao pelo crime informatico, mas pela ameaca, coisa que e' crime aqui tambem no Brasil.

Portanto, fiz uma coisa diferente, que foi arranjar para que o arquivo fosse enviado para a Freenet onde eu tinha conta e fiquei um tempo editando um arquivo de "alias" para fazer o envio. Usei como base uma lista de pessoas que estavam logadas na lista de hackers da Unicamp, a qual, por sinal, ainda nao tive coragem de perguntar pro administrador se ainda esta' funcionando. Isso porque eu recebia os arquivos que eu enviava para a lista, mas nao sabia de ninguem mais que estava logado e que recebesse esses arquivos. Pode ser por lentidao do sistema ou porque la' tambem nao gostam da lista..

E', pode-se dizer que a paranoia esta' comecando. Os responsaveis pelo break-in na USP de Sao Carlos me enviaram um mail, comentando o que acham do meu e-zine. Impressionante. O primeiro grupo de crackers a me mandar uma carta. Ainda bem que nao gostaram muito dele. Nao e' preciso muito para pensar que a minha conta atualmente deve estar sendo "checada", volta e meia. Eu faria isso, se fosse administrador do computador onde tenho conta. Um Sysop tem um nome a zelar. Ele e' um cara que pode ser despedido ou rebaixado, se for incapaz de administrar o sistema.

O mesmo acontece comigo e a minha carreira, se o meu nome for ligado a atividades criminosas. Nao e' legal? Mas paciencia. Vou continuar a divulgar minhas ideias, que vao mais pelo lado de conscientizar do que de fazer apologia de vandalismo. Porque tem um detalhe: quanto maior o numero de vandalismos, maior sera' a dificuldade de implantar isso no Brasil e o prejuizo sera' para todos, nao apenas para um ou dois usuarios.

A PESSOA DIGITAL

Quando voce entra com em possessao de um usercode e uma senha de acesso a um computador que tenha acesso a rede, ou a uma BBS de qualquer tipo, e voce passa a usar esse acesso, algo ocorre. Voce esta' entrando num ambiente onde so' aquilo que o teclado mostra interessa. A mudanca fica mais evidente quando voce faz parte de uma

conferencia tipo Chat ou IRC. Escolhendo um apelido, so' algumas pessoas terao inteligencia o bastante para descobrir se voce e' homem ou mulher, rico ou pobre, bonito ou feio. E essas pessoas dependerao do seu discurso no teclado para isso. Em outras palavras, como apareceu numa charge: " Na Internet, ninguem sabe que voce e' um cachorro".

Roger Clarke, descreveu essa pessoa digital como: " um modelo da personalidade publica do individuo baseada em dados e mantida por transacoes". Existe a personalidade que o individuo impoe na sociedade ou seja, a projetada e a outra, fruto daquilo que o individuo fez e ficou registrado, coisas como registro bancario, etc.

A tela de computador, ao contrario da vida real, permite construcoes de personalidade relativamente faceis. Uma pessoa pode frequentar meios digitais completamente diferentes, exibir comportamentos diferentes, sem grande dificuldade. Em "Neuromancer", a coisa vai mais longe: a pessoa digital e' gravada num cassete, e todas as suas respostas, obssessoes, e habilidades estao la'. Essa personalidade projetada poderia ser imortal.

Algo mais interessante e' o uso de "handlers" ou "nicknames". O cara que entra nesse universo tenta arrumar um nome ou apelido que substitua sua identidade real. Esse nome substitui o real e ao mesmo tempo passa uma vaga ideia sobre como voce e' ou o que voce faz. "Captain Crunch" foi um hacker famoso durante bastante tempo e o nome veio de um personagem de caixa de flocos de milho. O brinde era um apito que podia ser usado para "phreaking".

"Phiber Optik" ficou na historia do "Hacker Crackdown", pela sua habilidade. Mark Abene, seu nome verdadeiro. Fez varias demonstracoes sobre como "entrar" em bancos de dados de acesso restrito. Foi preso por fraude telefonica, coisa bastante simples perto do tipo de "cracking" que era capaz de praticar. Bastante conhecido dos jornais e revistas (colaborador da "2600 - Hacker Quaterly"). O juiz pronunciou mais ou menos a seguinte sentenca:

"Mister Abene, o senhor e' um simbolo para a comunidade hacker. Dessa forma, eu devo sentencia-lo como um simbolo. Mas o senhor deve cumprir a pena em pessoa."

Os dados arquivados sobre as interacoes do sujeito na sociedade compoem outro tipo de pessoa digital, a passiva. Essa e' composta nao e' composta da forma como a pessoa age, mas por exemplo, os newsgroups que ela frequenta, os horarios em que ela acessa a rede, com que tipo de assuntos normalmente lida. Em suma, dados pertinentes sobre a pessoa.

Vou usar um exemplo pessoal para colocar a diferenca:
A minha pess. digital projetada e' a minha personalidade, as pessoas sentem ao ver minhas cartas ou ao fazerem "talk" ou "chat" comigo.

O que eu faco, por outro lado, pode estar sendo monitorado por um programa qualquer. Os dados que eu coleto na rede, sistemas que eu acesso, mail que recebo, tudo isso sao dados podem ser relacionadas a coisas que eu fiz na rede. Esta' registrado. Eu nao posso mudar isso, porque nao tenho acesso aos registros. Essa e' a pess. digital passiva.

A partir do momento em que existem dados o suficiente sobre mim, um perfil pode ser tracado, e diferencas podem ser inferidas. Voce pode ser dessa forma, inserido num grupo ou subgrupo e ser tratado de acordo. Isso e' muito usado em pesquisa publicitaria, que tenta avaliar o publico para determinado produto.

Esse tipo de raciocinio, se formos ver a Internet, que nao tem o que chamamos de leis, mas antes regras de conduta, nao significa muito. Mas as empresas estao comecando a entrar na rede, em busca de mercados novos, na area de propaganda. E' prematuro ainda dizer que tal preocupacao em anotar os dados da pessoa ocorra.

Apenas existe o fato de que existe um passado digital que e' acumulado sobre o individuo que acessa a Internet ou qualquer BBS. Se voce acessa informacoes sobre crime por computador, aids, ou confeccao de boomerangs, tudo isso e' algo que pode ou estar sendo registrado em algum lugar. No Brasil, ja' houve o caso de um engenheiro que foi processado por colocar sua opiniao sobre um livro de MSDOS. O editor do dito leu a mensagem do cara e entrou com um processo por perdas e danos. Outro cara la' nos EUA usou um nome real numa historia ficticia e levou outro processo.

Nao e' pelo fato de estar por tras de um modem e de um computador que as coisas nao podem acontecer com voce. Para quem nao sabe o que isso significa, nem nunca morou em ambientes onde a fofoca pode trazer prejuizo, vou dar um exemplo comum:
Vamos supor que voce foi pego fumando maconha. Podia ser sua primeira vez. Se foi seu pai que foi te tirar da policia, a coisa ate' poderia parar ai'. Ficaria em familia. Mas se voce foi preso com outro cara, mais antigo na coisa e a noticia espalhou. Quem conta um conto aumenta um ponto e subtamente, voce e' "o maconheiro". Voce tem passagem na policia. Os seus amigos tem entao duas opcoes, a de continuar seus amigos ou de te esquecer. Porque quem aparecer com voce, pode correr o risco de ser rotulado tambem como maconheiro, (Diga-me com quem andas e te direi quem es) e sujeito a desconfianca paterna, na hora de emprestar o carro ou pedir dinheiro (e' para comprar o que).

OBS: O exemplo pode parecer meio besta, mas muita gente comenta o caso de um politico brasileiro que perdeu as eleicoes por conta do fato de ter assumido que ja' tivera experiencia com a coisa. Por essas e outras, estou colocando uma resenha do livro "1984", de George Orwell. O livro e' ficcao, mas para nos latino-americanos, ja' foi e qualquer dia pode voltar a ser realidade. Basta ver o caso do Peru, que implantou a ditadura, para ver se escapava da ameaca de um movimento campones que poderia significar tambem outra ditadura.

1984 - O LIVRO E NOSSA PRIVACIDADE

George Orwell escreveu esse romance durante a Segunda Grande Guerra, revoltado com o que julgava ser um palco de hipocrisias gigantescas. O livro conta, basicamente, como um funcionario do governo, que se apaixona por uma colega de trabalho acaba sendo preso por crimideia, ou crime por pensamento.

No mundo relatado por Orwell, nao existem leis. Mas qualquer coisa que nao for aprovada pode significar a prisao. O interessante, e' que todo mundo esta' sendo vigiado pelas tele-telas, aparelhos de tv que permitem que o individuo seja escutado e observado, enquanto assiste sua programacao. Microfones estao por toda a parte, e ate' existe um projeto de criacao de uma nova linguagem, que tornara' o crime de pensamento impossivel.

Em suma o livro e' uma descricao sobre como o aparato tecnologico pode ser usado para escravizar o homem. E' pesado de ler, principal-mente quando se sabe que situacao semelhante aconteceu no Brasil, durante o regime militar. As pessoas nao se davam conta da ditadura, por causa do fato de que havia uma imensa maquina de propaganda, controlando a opiniao. A imprensa era censurada. Professores nao sabiam se um de seus alunos nao era um informante do SNI.

No tempo em que foi escrito, existia varios tipos de regime totalitarios, como o Nazismo, o Facismo, o Comunismo e suas variantes.

Por isso, era relativamente facil se descrever tal tipo de situacao. O radio comecava a ser usado como forma de distribuir o pensamento politico do governo e tanto na Alemanha como na U.R.S.S., uma crianca podia mandar seus pais para campos de concentracao, ao "dedurar" uma ou outra opiniao politica discordando da vigente. Todos estavam sendo vigiados para possiveis crimes ou "atos de sabotagem".

Esse e' um livro que merece ser lido, por qualquer um que pretenda ter uma opiniao sobre o futuro. Ainda que nao exista mais um regime comunista, nao impede o uso das mesmas tecnicas, em lugares inesperados, como nosso ambiente de trabalho. Estamos vivendo numa epoca em que a informacao esta' cada vez mais facil de acessar. So' para fechar, o livro e' leitura obrigatoria no curso secundario dos EUA. Deu origem a varios outros no mesmo estilo, como "Laranja Mecanica" - Anthony Burgess, e pode-se perceber a influencia em outras obras, como o filme "Blade Runner" e o livro "Volta ao admiravel mundo novo", de Aldous Huxley.

Explicar a fixacao de hackers, crackers e outros por esses livros e' simples: eles colocam o fato de que cada vez mais, estamos entrando num universo semelhante ao retratado neles, em que a opiniao pessoal e' substituida pela opiniao da midia. Para quem nao sabe, na Tailandia, as pessoas vao ter um unico documento: um cartao magnetico com a foto do sujeito e dados pertinentes. Oba! E', toda a papelada que existe sobre voce sera' substituida por um arquivo, armazenado num computador central existente em algum lugar. Um arquivo que pode ser apagado por um virus de computador (voce deixa de existir como pessoa fisica e cidadao) ou erroneamente manuseado (como no filme "Brazil").

Ate' um tempo atras, para se usar um motel, o sujeito preenchia uma ficha, como em qualquer hotel. Ai' descobriu-se que acontecia, era pratica talvez da policia, entrar no estabelecimento, pedir as fichas sobre pretexto de procurar um suspeito, e anotar o nome do pessoal casado (acompanhado de gente solteira). Depois esses elementos, iam na casa do sujeito pedir um dinheiro para nao abrir o jogo com a companheira do cara. Isso faz muito tempo, e logico que nao podemos supor que as coisas sempre aconteciam desse jeito. Nem todo mundo e' corrupto a esse ponto. Mas o sistema de registro de moteis de alta rotatividade foi alterado.

Nos EUA, esse tipo de coisa vai mais longe. Se voce vai num medico se consultar, ele anota dados a seu respeito. Esses dados vao para uma ficha medica, que e' armazenada numa instituicao. E ficam fora do alcance do individuo para alteracoes, mas dentro do alcance de empresas, para consulta. Uma funcionaria teve o pedido de licenca medica negado, sob a alegacao de que o motivo alegado era irrelevante, diante da ficha medica. Outro, foi mal interpretado pelo medico, que anotou um consumo abusivo de bebida na ficha do sujeito, atrapalhando sua vida para uma serie de coisas, inclusive ao mudar de emprego (historico de alcoolismo, estas coisas).

Na revista Super-Interessante, num artigo ate' interessante sobre isso, o exemplo real sobre um bancario, que ao chegar a chefe de sindicato, foi alertado para o perigo de um cheque sem fundo, motivo para demissao por justa-causa. Num banco, sempre se sabe quando houve uma festa num buteco e quem participou, pelos cheques que sao depositados na mesma conta. Aqui no Brasil nao sei, mas nos EUA, todo mundo usar cartao de credito, e pelo historico do cartao de credito sabe-se todas as despesas que a pessoa tem. Com que, quando e como.

Hoje, no Brasil, esse tipo de coisa e' uma curiosidade. Amanha, pode acontecer com voce, ver o seu passado vasculhado em busca de algo que possa ser usado, mas nao para seu beneficio.

BRINCANDO COM CRIPTOGRAFIA

Criptografia vem do grego cryptos (escondido) + grafia (escrita). Uma coisa que volta e meia aparece na rede Internet sao discussoes sobre esse tema, normalmente envolvendo a questao do PGP e do chip Clipper. Essa preocupacao ocorre porque o americano tem embutido na Constituicao o direito a privacidade. O brasileiro e' ligeiramente diferente. Ele so' se preocupa com o direito a privacidade quando vai fazer algo que nao quer que os outros saibam, tipo trair a mulher ou sonegar dinheiro do imposto de renda. So' que nesses casos, varias vezes a coisa da' errado, porque e' feita de forma amadora, acaba dando problema pela inexperiencia da pessoa. O gosto pela criptografia como um passatempo nao e' algo difundido, da mesma forma. O brasileiro acha mais interessante o misterio do que a descoberta. Existe a paixao por palavras cruzadas, que engloba tambem cripto-analise, mas nao a de cifrar e esconder mensagens, a nao ser na nossa querida musica popular e outras formas de expressao popular durante os periodos "negros" do pais.

Na verdade, talvez pela ditadura, talvez pelo fato de que o brasileiro teve o acesso as letras (crescimento do parque industrial necessario a impressao e distribuicao de livros a precos populares) mais ou menos durante o tempo em que o radio e a televisao faziam sua estreia aqui no Brasil. O maior estimulo contra o analfabetismo, que seria a ansia de ler noticias do jornal ou novelas e romances de aventura, foi sendo preenchido pela TV. O que nao aparece na Globo, nao existe. Um analfeto sobrevive perfeitamente na nossa sociedade, com um misero aparelho comprado num camelo. Dai, como entender algo tao sutil, como arrumar razoes para se interessar por criptografia ou criptoanalise? Existem pessoas cuja grafia faria qualquer medico se morder de inveja. As vezes a propria pessoa nao entende o que escreve.

Durante os periodos da ditadura, coisa que e' quase moda acontecer aqui no Pais (basta ler um pouco de historia), havia a censura aos meios de comunicacao. Nao podia se dar o nome aos bois, nao podia se falar palavras indevidas, nao podia se contar o que estava acontecendo. O reporter que quisesse dar um colorido a sua materia ou transmitir algo diferente, de conteudo mais ideologico ou subversivo tinha que mascarar o conteudo, para ver se "driblava" o censor, mas nao o leitor. Se a noticia fosse muito forte, podia acontecer de toda a tiragem do jornal ser pura e simplesmente confiscada. E' facil de encontrar lembrancas desse periodo, basta procurar em livros antigos, a mensagem "texto integral, sem cortes". Para garantir a vendagem dos jornais, durante o periodo da ditadura, alguns editores comecaram a editar receitas culinarias. Imagina jornais, do porte do Estado de Sao Paulo ou o Globo fazendo isso:

Na primeira pagina, ao inves de uma noticia sobre a queda de um ministro: "Rabada 'a moda Magri - Primeiro pegue uma carne de segunda ou de terceira, guarde o caldo, misture com um molho Volnei...". Algumas vezes, os leitores escreviam cartas reclamando que as receitas nao funcionavam, apesar do aviso de que essas receitas nao significavam absolutamente nada. E o pior e' que os jornais duplicavam a receita, quando imprimiam este tipo de coisa. Na musica popular, isso acontecia muito tambem, ate' a mocada ser obrigada a se asilar, antes de enfrentar cadeia. Dizer que determinado artista queria ou nao transmitir essa ou aquela mensagem e' algo meio forte. Mas era proibido abordar uma serie de temas, durante aquele periodo do milagre brasileiro, como a pobreza ou a repressao. So' pra se ter uma ideia, durante o bicentenario da independencia dos EUA, comemorado em 1976, foi proibida a publicacao de trechos da declaracao dos direitos do

homem nos meios de comunicacao (coisas como "Todo homem tem direito a liberdade de opiniao e expressao" eram consideradas subversivas).

Pode-se encontrar montes de mensagens de duplo sentido, na musica daquele tempo. Na literatura, o romance Zero, do Ignacio de Loyola Brandao, um verdadeiro diario de um "terrorista", passou incolume pela censura (virou um sucesso de vendas e..foi proibido depois que esgotou, porque descobriram o lance).

Okay, eu contei a historia de varios exemplos de *codificacao* de conteudo de uma mensagem, mas nao de criptografia. Existe um grupo de discussao sobre isso (em portugues), na esquina-das-listas e existem varios em ingles, como o sci.cript, sci.crypt.research, etc. Os FAQs (Perguntas mais frequentemente respondidas - documento introdutorio) desse grupo e' uma fonte de referencia muito boa, e nao tenho muita *intencao de substituir, mas aqui vai um vocabulario para os iniciantes que queiram depois se aprofundar:

TEXTO PURO: E' o texto destinado a ser colocado de forma secreta ou ininteligivel para o publico comum.

TEXTO CIFRADO: E' o texto puro apos ser alterado pela cifra ou palavra-chave.

CIFRAR, CODIFICAR: Ato de transformar o texto puro em texto cifrado.

DECIFRAR, DECODIFICAR: Ato de transformar o texto cifrado em texto puro.

QUEBRAR A SENHA OU SEGREDO: Conseguir decifrar um texto cifrado sem possuir a senha.

COMPACTACAO DE ARQUIVOS: Metodo de reduzir o espaco ocupado em bytes por um arquivo armazenado em computador. Alguns programas que realizam esse trabalho tem opcao de criptografar o conteudo com uma senha escolhida pelo usuario.

ESTENOGRAFIA: Sobre as formas de se ocultar ate' que a mensagem existe. Metodos como sublinhar a primeira letra de cada palavra do texto ou produzir um texto de tal forma que suas primeiras letras tenham uma mensagem.
(exemplo: Quem assistiu a novela "Guerra dos Sexos" pode especular se a personagem Francisca Moura Imperial nao era uma forma de fazer referencia ao FMI, que como a personagem, controlava a economia brasileira).

TRANSPOSICAO: Alterar a ordem das letras, tal como tranformar segredo em esoderg.

SUBSTITUICAO: Substituir letras especificas por outras, ou por numeros ou simbolos. Escrever SOS em codigo morse seria uma substituicao.

ex: texto puro: SOS codigo morse: ...---...

Varios musicos tambem usavam linguagem de
duplo sentido, para poder transmitir sua mensagem (isso, antes de terem que se asilar para escaparem a repressao).

ALFABETO CIFRADO: Um alfabeto para ser usado para transposicao.

ex:

Alfabeto puro: a b c d e f g h i j k l m n o p q r s t u v x y z

Dessa forma, inimigo viraria TQTPTCE. Pode-se usar mais de um alfabeto, quando entao o sistema se chama polialfabetico.

CODIGOS: Essa e' mais ou menos, a forma favorita do brasileiro de cripotografia. Consiste em se utilizar palavras-de-codigo ou numeros-de-codigo para representar o texto, como acontece com as girias.

ex: numero-codigo	texto-puro
11	muito bom (ver filme "mulher nota 10")
10	bom
1	ruim
5	medio
24	homossexual
171	estelionato

Obs: Usei exemplos ja' incorporados a cultura popular, mas esse tipo de codigo e' muito usado pela policia. A giria usada por um grupo especifico, tal como usar "foca" para designar reporter iniciante na imprensa tambem pode ser chamada de codigo.

VOCABULARIO: Nesse texto, o conjunto de palavras que compoem um codigo, tal como visto acima.

PALAVRA-CHAVE: A expressao ou codigo que permite o deciframento do texto cifrado.

HISTORIA:

A criptografia e' algo bastante antigo, tao antigo quanto a escrita. Era usada no antigo Egito e na Mesopotamia. No Kama-Sutra, e' citada como uma das 64 artes, ou yogas, que a mulher deveria conhecer e praticar. Na Grecia antiga, o que hoje conhecemos como civilizacao ocidental teria sido extinto se nao fosse uma mensagem criptografada avisando da invasao persa. O episodio dos "300 de Esparta" nao teria acontecido, porque os gregos nao teriam sido avisados em tempo.

Julio Cesar tambem relatou o uso de mensagens cifradas em seu livro, sobre as Guerras Galicas. Seu nome foi dado a qualquer tipo de alfabeto cifrado semelhante ao que usou:

alf. puro:	a b c d e f g h i j k l m n o p q r s t u v x y w z
alf. Cesar:	D E F G H I J K L M N O P Q R S T U V X Y Z A B C D

Pulando alguns seculos, Leonardo da Vinci escreveu seus projetos, na epoca mirabolantes (e passiveis de serem premiados com um churrasco promovido pela Inquisicao) atraves da escrita em forma reversa. Podia ser lida colocando-se o original de frente a um espelho.

Nostradamus foi outro que tambem se preocupou com a possibilidade de virar churrasco e desenvolveu suas centurias numa linguagem que ate' hoje tenta se descobrir. Descobre-se o que ele estava falando depois do acontecido, na maioria das vezes. Os alquimistas, de forma geral, ficaram bastante conhecidos por escreverem suas receitas de forma cifrada, durante a idade media.

Ja' mais recentemente, no inicio do seculo, varios situacoes na historia tiveram o seu curso alterado gracas ao bom (ou mal) uso da criptografia. Os alemaes, na primeira guerra venceram os russos facilmente, por conta disso. Os EUA conseguiram nao perder do Japao na

Segunda Guerra por possuirem os codigos de transmissao deste. Os alemaes, por sua vez, nao conseguiram invadir a Inglaterra pelo mesmo motivo. Rommel deve sua fama de raposa do deserto em parte ao fato de que conseguiu capturar uma transmissao americana detalhando como era o modo de operacao dos britanicos no deserto.

Nao e' a toa que os EUA tem uma agencia devotada ao estudo de codigos criptograficos, conhecida como NSA. La' no norte, para sair do pais com um telefone celular contendo mecanismo de codificacao, e' necessario permissao especial, ou a pessoa e' enquadrada numa lei feita inicialmente para prevenir o contrabando de armas. Se voce entra com um mecanismo desses nos EUA, ao voltar com ele voce pode ser preso. Quem nao acredita, pode ver o caso Zimmerman, que desenvolveu o PGP. O fato dele ter colocado o programa como freeware, disponivel na Internet, tornou-o um criminoso.

Existem muitos casos em que a criptografia e' usada, como em empresas que querem proteger seus segredos de espionagem industrial, quando transmitindo por via telefonica ou telegrafica. Existiam livros de codigos especificos para tambem se poupar dinheiro com transmissoes telegraficas, quando este era o modo mais completo de comunicacao. Dessa forma, frases inteiras eram substituidas por uma palavra, (mais ou menos como o carioca fala, resumindo numa palavra, coisa que levaria varias frases: Pergunta "Cade fulano?" Resposta: "sifu." Disse tudo) e estes eram chamados de codigos comerciais.

O melhor livro para se ler sobre criptografia e' o "THE CODEBREAKERS", do autor americano David Kahn. Um livro para macho. 1127 paginas em ingles. No que se refere a historia da coisa, e' obrigatorio.

Lendo o livro, fica-se boquiaberto em saber que existiam ja' clubes dedicados ao estudo dessa materia como hobby na maioria dos paises civilizados, desde o inicio do seculo, mas nao no Brazil, que so' aparece como referencia quando se fala que pais XXX conseguiu decodificar o codigo diplomatico de pais YYY, e do Brazil. Quando se imagina o problema estrategico que isso representa, e' de se estranhar como e' que nao se pensa mais nisso.

Poderia se acrescentar por exemplo, que no periodo Sarney, um radioamador conseguiu fazer a escuta do telefone celular do presidente em seu sitio, e esse se recusou a instalar um dispositivo de seguranca mesmo apos saber pela imprensa da falha. No caso PC-Farias, foi muito criticada pela comunidade de seguranca informatica, o uso tao pobre de criptografia num sistema de valor tao alto (ainda bem).

TECNICAS SIMPLES:

TRANSPOSICAO:

Ordem Reversa:

A mensagem e' escrita de tras para frente. Em seguida, reune as letras em novos grupos.

Texto Puro: Seu marido vai embora quando?

(1) odnauq arobme iav odiram ues?
(2) od nauqa rob me iavod ram ues?

Texto cifrado: od nauqa rob me iavod ram ues?

Bi-reverso:

As letras sao agrupadas em pares e os pares tem a ordem invertida.

Texto Puro: seu marido vai embora quando?

(1) (se) (um) (ar) (id) (ov) (ai) (em) (bo) (ra) (qu) (an) (do)
(2) (es) (mu) (ra) (di) (vo) (ia) (me) (ob) (ar) (uq) (na) (od)

Texto cifrado: esmu radi voiame obar uqna od

Grupo reverso:

As letras sao divididas em grupos que sao colocados em ordem reversa.

Texto Puro: seu marido vai embora quando

(1) seuma ridov aiemb oraqu ando
(2) amues vodir bmeia uqaro odna

Texto Cifrado: amues vodir bmeia uqaro odna

SUBSTITUICAO:

Alfabeto cifrado:

Alfabeto Cesar. Como se pode ver, o alfabeto comeca na letra D, mas poderia comecar em qualquer outra. As letras iniciais sao colocadas depois da letra Z.

alf. puro: a b c d e f g h i j k l m n o p q r s t u v x y w z
alf. Cesar: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Ex:

Texto puro: ganhei na loto
Texto cifr: jdqkhl qd orwr

Observacoes: A partir desse metodo, pode-se colocar mais de um alfabeto, para dificultar a critpo-analise. Quando a mesma letra se repetir, usa-se a segunda cifra. Essa e' a cifragem por substituicao multipla.

alf. puro: a b c d e f g h i j k l m n o p q r s t u v x y w z
alf. Cifr1: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Alf. Cifr2: F E G D J H I M K L P N O S Q R V T U Y W X B Z A C

Texto puro: ganhei na loto
Texto cifr: jdqkhl sf orwq

TRANSPOSICAO:

Este metodo, projetado pelo grego Polybius, e' anterior a Cesar, mas continua difundido como metodo de criptografia. Funciona se ajuntando as letras do nosso alfabeto num quadrado 5X5. Para nao complicar, a letra K e' retirada e substituida por C:

```
      1    2    3    4    5
    -------------------------
1   I a    b    c    d    e
```

2	I	f	g	h	i	j
3	I	l	m	n	o	p
4	I	q	r	s	t	u
5	I	v	x	y	w	z

Dessa forma, a letra E passa a ser representada por 15, a letra O pelo numero 34 e assim por diante.

TECNICAS DE CRIPTOANALISE:

Para praticar, o ideal sao palavras cruzadas. Mas para tentar decifrar um texto feito com um dos metodos acima, sem saber qual, ha' varias formas.
Primeiro e mais importante e' nao trabalhar com o texto original, mas fazer uma copia com espaco entre as linhas, para se trabalhar. Depois procurar as vogais, que estao presentes em todas as palavras. As consoantes duplas como ss e rr sao outro bom alvo. Outras combinacoes comuns de letras sao lh, ch, nh, br, cr, dr, gr, pr, tr, bl, cl, fl, gl, pl, tl.
Saber sobre o que o texto fala pode ajudar, assim como ajuda saber o destinatario da carta. Palavras como amanha, que repetem a letra a varias vezes, tambem sao bons indicadores.

OBSERVACOES:

Na verdade, todos os metodos acima estao bastante obsoletos. Poderia ate' colocar um programinha em C ou Basic para implementa-los, mas acho besteira. Quem souber um pouco de Word for windows nao tera' dificuldade em fazer uma macro tanto para cifrar como para decifrar. Sao interessantes porem, porque sao simples e faceis de usar, o que pode ser interessante para praticar. Com estes elementos basicos podem se projetar outros mais complicados.

METODOS MAIS AVANCADOS E FRAQUEZAS:

Existe centenas de metodos de criptografia. Alguns famosos, como o Playfair, o Vignere, e as cifras de utilizacao unica. Muito poucos resistem a um bom cripto-analista. Hoje em dia, a criptografia e' feita tanto via hardware como software. O programa Unix carrega em si um programa de criptografia, chamado CRYPT. Ja' existe software que permite, com um pouco (medio) trabalho, decifrar textos cifrados por ele. Outros softwares, como o WordPerfect, versao 5 (a 6.0 eu nao conheco) tem opcao para criptografar os documentos. Funcionam, mas qualquer conhecedor de BBSes ou de sitios FTP como o Simtel 20, ja' viu referencia a um programa que "quebra" a senha do arquivo criptografado dessa forma.

O unico programa com uma fama de ter a criptografia dificil de quebrar e fartamente disponivel ao publico e' o PKZIP204G. Trata-se de um compactador de arquivos, com opcao -s. Existe o HPACK, outro compactador menos cotado, mas teoricamente ate' mais eficiente, bem pouco conhecido. O ARJ, ate' a ultima versao, tem a reputacao de ser facilimo de ter seus arquivos criptografados "quebrados". Existe o programa DISKREET, que vem junto com o Norton Utilities, mas nao ouvi muitas coisas a respeito dele. Parece facil de usar.

Isso sem falar no uso do metodo de "Forca Bruta", que ja' mencionei no numero anterior. Nesse caso, usa-se uma versao do programa e vai se usando senhas possiveis ate' se encontrar aquela que

destrava o arquivo. Pode-se ate' fazer um programa que faca a busca de todas as senhas possiveis. Teoricamente, a quantidade de tempo para se achar a senha aumenta geometricamente de acordo com o numero de letras usadas, sendo que qualquer senha com menos de 6 letras ou numeros e' considerada relativamente facil de quebrar.

O metodo de criptografia mais inteligente ate' agora e' o PGP, vulgo Pretty Good Privacy. O autor tinha o interesse em trazer a criptografia para as massas e desenvolveu um metodo atraves do qual qualquer pessoa, com um minimo de treinamento, pode ter sua privacidade garantida. O codigo fonte do programa esta' disponivel em varios lugares, e e' de dominio publico.

PGP - PRETTY GOOD PRIVACY

Achar que existe ou nao uma utilidade para um software que criptografa arquivos e' algo pessoal. Pode ser um caso amoroso, pode ser os numeros de uma conta numerada na Suica, pode ser um diario, pode ser qualquer coisa que voce nao quer se arriscar a que ninguem veja. Se certificar do segredo, usando um software que talvez nem uma agencia americana, como o NSA, uma especie de primo da CIA, seja capaz de decifrar e' algo diferente. E' preciso ter um tipo de preocupacao que pode ate' ser paranoico. Afinal de contas, nao basta um cofre forte? Porque alguem se daria ao trabalho?

Para que gastar talvez uns 10, 20 minutos se preocupando em criptografar horas de trabalho que podem tambem ser destruidas por um virus de computador? Se o problema e' perseguicao por forcas criminosas, nada impede que o conteudo do arquivo seja recuperado de outras formas, talvez ate' pela violencia, ja' que se fala em neurose.

Voce usa Correio Eletronico para se comunicar. Mas seus parceiros ou colegas de bate-papo, nao sabem seu endereco, nao sabem seu telefone, voce nao tem um canal seguro de comunicacao com eles. Nao pode estabelecer um codigo atraves do qual eles entendam aquela dica que voce recebeu anteotem de comprar dolar ou investir em cavalos. Tudo bem, voce pode enviar por correio normal, mas e se a namorada ou namorado da pessoa descobrir que voces se comunicam. Mesmo que seja estabelecido um codigo entre as duas partes, num dia qualquer, como e' que fica, quando outra pessoa finalmente acha a solucao para o enigma? Outro encontro privado? O problema sempre volta. Ontem, a Embratel queria controlar a Internet no Brasil. De uma hora para outra, BBSes tiveram seus contratos de uso da rede cancelados. Se isso torna a acontecer, como enviar aqueles quinze disquetes contendo a folha de pagamento da sua empresa pelo malote, sem temer violacao?

Se voce se torna famoso, e alguem quer lhe fazer uma proposta interessante, mas discreta, como enviar uma mensagem, que so' o destinatario podera' ler? A partir desse numero de possibilidades, pode-se ver que nao e' so' um paranoico que deseja ter privacidade, coisa cada vez mais dificil, num mundo cada vez mais cheio de gente. E nao pense que se voce tem uma conta na Internet, voce nao pode ter sua correspondencia lida. O Sysop ou super-usuario, tem poder de ler todas as cartas. Ele nao precisa nem mesmo ler todas ele mesmo. Existem programas que fazem isso, chamados de "sniffers". Mesmo um comando GREP do Unix pode ser feito de forma a procurar palavras-chave, dentro de seu arquivo. Mesmo que hoje voce acha ridiculo se preocupar com gente bisbilhotando sua vida pessoal, pense no seu amanha, quando a necessidade aparecer. Voce nao e' o Principe Charles, mas se sua mulher ou namorada resolver agir como Lady Diana, voce vai lamentar nao ter pensado em ter seus segredos guardados num cofre.

O Programa PGP foi desenvolvido por Philip Zimmerman, por volta

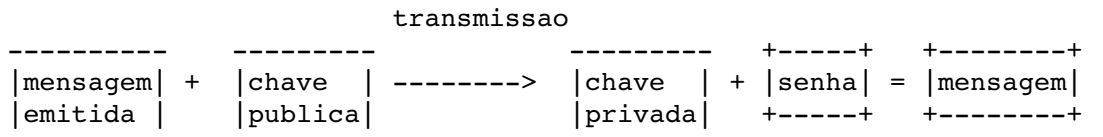
de 1990, apos uma longa pesquisa, sobre como resolver varios problemas que sempre plaguearam aqueles que se interessaram por proteger seus dados atraves da criptografia. O nome do programa vem de "Pretty Good Privacy", ou numa traducao mais livre: "Privacidade da Boa..".
Nos EUA, a palavra privacidade e' algo parte da constituicao. O homem tem direitos alienaveis, pelos quais ate' hoje se luta e se discute. Philip tinha essa preocupacao, tipica de um grupo da rede que se denomina de "Cipher-punks". Aqueles que nao querem que outros sejam capazes de vasculhar ou descobrir algo sobre suas vidas. O motivo ideologico e' esse. Talvez o outro motivo seja um gosto pela arte da criptografia, que e' uma especie de hobby em varios outros paises, mas o fato e' que por varias razoes, desde garoto o Philip matutou em cima de varios aspectos sobre cifras e codigos e aquela coisa de livros de espionagem. Depois de muita busca (ja' que material sobre o assunto tende a ser classificado como top-secret) e alguns anos de estudo, ele chegou a algumas conclusoes:

Um metodo de criptografia totalmente novo, sempre e' possivel de se quebrar, quando se leva em conta uma instituicao com grandes recursos ou outra pessoa com inteligencia e tempo o suficientes. Tudo o que um homem fez, outro pode repetir. Quando se mensagens cifradas, depende-se de uma cifra, ou metodo de codificacao, da qual ambas as partes devem possuir. Se este for quebrado ou violado de alguma forma, pode-se levar muito tempo para o desenvolvimento de outro. Metodos de cifragem "perfeitos" podem levar horas para serem usados (no caso dos antigos metodos, que usavam lapis e papel) e podem ser dificeis de serem aprendidos. Outros metodos simples e rapidos de serem usados, por mais sofisticados ou novos, podem ser "quebrados" por um estudante de palavras cruzadas que tenha alguma nocao do conteudo. E por ultimo, todo criptologista cedo ou tarde chega a conclusao, alguma hora, de que inventou um metodo "perfeito" e "impossivel" de ser decifrado.

Tudo isso acima e' quase que basico na criptologia e na cripto-analise. Zimmerman descobriu que seu metodo "perfeito" era exercicio basico para estudantes de cripto-analise, numa ocasiao. Ja' haviam os codigos comerciais, postos a venda para empresas e firmas que precisassem deles. Mas ainda assim, eram codigos vulneraveis. Sera' que so' os governos seriam capazes de ter direito a ter documentos passiveis de continuarem secretos? Haveria um jeito do cidadao comum ter o direito de manter seus escritos ininteligiveis para os outros a sua volta? Afinal de contas, se um codigo esta' a venda, varios podem decifrar aquilo que fulano aprendeu a criptografar.

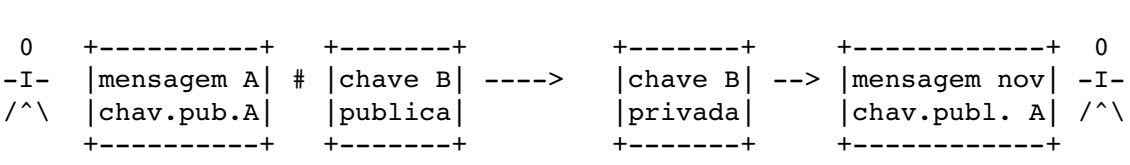
O PGP foi feito apartir de um algoritimo, chamado RSA (as iniciais dos inventores) e um conceito de dupla chave. Uma ideia simples, mas que cobre quase todas as fraquezas que um sistema de seguranca poderia ter. O metodo se baseia na existencia de duas chaves, de criptografia. Um metodo normal teria uma senha ou conjunto de numeros atraves do qual o(s) arquivos de dados seriam criptografados ou descriptografados. Mas essa senha teria que ser distribuida atraves de um canal seguro de comunicacao. As embaixadas usam "Couriers" ou pessoas de alta-confianca para a entrega dessas senhas, que sao escoltadas durante o trajeto. Nem sempre isso e' possivel, para o cidadao comum.

O metodo do PGP se baseia na ideia de uma chave (senha) publica de criptografacao, que nao serve de forma alguma para reverter o processo. Essa chave, e' ainda distribuida atraves de um canal que pelo menos assegure a origem (ja' que nao deve ser alterada ou substituida antes de se encontrar o destinatario final). A mensagem, uma vez entregue no destino, sera' decifrada pelo programa com uma outra chave, privativa do usuario, que precisara' tambem de uma senha, sem a qual o programa nao inicia o processo.



Tudo bem, mas e se algo acontece e a pessoa nao se lembra da senha, a mensagem esta' perdida e todas as outras seguintes tambem estarao. Nao. A pessoa pode enviar uma mensagem revogando a chave-publica, para todas as pessoas que ainda tem uma copia dessa chave. Elas esperariam uma mensagem contendo a nova chave. E como seria possivel que essa mesma chave nao fosse distribuida a pessoas erradas, que a usariam ou tentariam adulterar.

Tudo bem. Mas a questao e' que nesse caso, duas pessoas que se comunicam tem cada qual, a chave-publica da outra. O problema que uma delas tiver afeta todo o conjunto chave-publica+senha+chave-privada, de modo que a pessoa nao pode mais decifrar mensagens que recebe. Mas ela pode enviar mensagens, pois a outra pessoa nao tem o mesmo problema. O conjunto chave-publica+senha+chave-privada pode ser re-feito. Uma nova chave-publica revogando a anterior pode ser enviada para o destinatario, do ponto de vista tecnico, vai simplesmente decifrar o arquivo, e copia-lo para usar na proxima correspondencia.



E' mais facil de entender quando se pensa que apesar do programa usado por A e B ser o mesmo, ambos tem senhas diferentes. Quando um fica com sua senha avariada, a situacao e' a do sujeito ao telefone que so' pode falar, mas nao ouvir. Ao enviar uma nova chave-publica p. B, este aprendeu como falar de forma que A pudesse entender a mensagem.

Mil e umas possibilidades existem, usando esse principio basico, sem comprometimento da seguranca. Cada chave-publica apresenta uma especie de certificado, que e' tambem garantia contra uma adulteracao.

Como os arquivos contendo as chaves sao arquivos txt, podem ser copiados ate' sem o conhecimento do remetente e destinatario, mas como e' necessario o arquivo contendo a chave privada + a senha (que pode ser uma frase que so' o destinatario conheca) para a mensagem ser decifrada, o processo e' seguro. Mesmo que a chave privada desapareca, ainda sera' necessaria a senha.

Fim da historinha de Zimmerman e lugares para se conseguir o PGP

A NSA (National Security Agency) considerou o PGP um atentado ao monopolio da criptografia exercido por ela. Zimmerman queria que o metodo fosse distribuido as massas. Por isso colocou a versao inicial do programa como dominio publico, significando que qualquer um usar o dito para qualquer fim, ate' para conseguir dinheiro (parece que so' uma companhia e' que ficou com uma licenca para ate' vender, mas isso, dentro dos EUA). A questao e' que a primeira patente do algoritimo utilizado, o RSA e' americana. So' para se ter uma ideia, esse tipo de patente nao e' exportavel. Se voce sai dos EUA com um telefone contendo equipamento de embaralhamento de voz sem uma licenca (para

alguns materiais criptograficos eles dao licenca, para outros nao) de exportacao, voce e' preso por um artigo de uma lei usado para coibir contrabando de armas. E'. Tao querendo enquadrar o Zimmerman nessa por ter colocado esse programa na Internet. Foram lancadas varias versoes, ate' se chegar a 2.3, que foi lancada a partir da Australia. Com codigo fonte e tudo. Nisso o processo ja' tinha comecado, existe ate' um movimento para arrecadar grana para o Philip nao encarar uns anos de "chumbo", senadores falando contra e a favor, um aue^ judicial, ja' que embora por lei ele esteja limpo, as pressoes por parte do governo sao para torna-lo um exemplo de quem se mete no que e' privativo do governo.

Foi lancada a versao 2.6 e depois a versao 2.6.2, usando algoritimos diferentes, desenvolvidos fora dos EUA, portanto iriam mais ou menos aliviar a "barra" no que se refere ao algoritimo RSA (que era patente do governo). Do lado de fora, no exterior, o pessoal ficou tao entusiasmado que criou sua propria versao do PGP, baseada no codigo fonte da versao 2.3. Eu nao entendo como isso acontece, mas a versao 2.6i - i de internacional - entende mensagens cifradas com a 2.6 americana e vice-versa. Sao equivalentes. Existe o barato de que usar a 2.6 pode ou nao implicar que voce fez um "download" ilegal dos EUA. O americano que quiser fazer o download desse programa atraves da Internet passa por uma burocracia para provar que e' americano e que faz isso a partir dos EUA (senao e' crime e pode ser processado). Dentro desse contexto, entrar e sair dos EUA com um disquete contendo isso pode dar cana la', mas essa lei nao vale aqui. So' que ao difundir a chave publica vai junto a versao atraves da qual a dita foi feita. De vez em quando, um moralista pode te inquerir acerca disso na rede e falar para voce mudar da 2.6 para a 2.6i. So' que se voce tem como provar que nao e' responsavel pelo contrabando da dita, ja' que todo mundo ja' tem, essa historia toda deixa no ar um cheiro de frescura enorme. Ate' os americanos admitem isso. Mas lei e' lei. E eles levam a serio e se voce pretende ir ate' la', e' bom respeitar.

Bom, para fazer o download do dito. A ftp.eff.org tem um subdiretorio explicando o procedimento para quem e' americano. A pessoa faz ftp para um lugar x, com uma senha enviada por e-mail. Como estou escrevendo isso para os brasileiros:

Existem os seguintes sitios ftp

ftp.demon.co.uk
ftp.informatik.uni-rostok.de
ftp.dsi.unimi.it

E' necessario procurar por um subdiretorio pub/crypt ou pub/crypto. Para quem nao acha isso o suficiente, procure na Usenet o newsgroup News.Answers. La' provavelmente voce encontrara' um FAQ sobre onde achar o programa (alem de outros faqs interessantes).

Observacoes finais:

O ideal seria nao pegar a versao 2.6.2, ja' que as versoes 2.6 e 2.6i vao estar funcionando por um tempo ainda razoavel, mesmo se a gente esquecer que tem algo de ilegal em usar a ultima versao. Dentro da dita vem os arquivos PGPDOC1 e 2 detalhando o uso. O ideal e' ler umas tres ou quatro vezes e ao fazer a primeira chave publica e privada, apagar tudo e repetir o processo, ate' ter certeza que aprendeu. Se for usar o arquivo em ambiente Unix, acrescentar -a para obter um arquivo em ASCII, que possa ser enviado em mail. Existe versao do PGP para Unix, mas se voce nao for o Sysop, isso nao ira' garantir

seguranca da correspondencia enviada a voce.

ENDERECOS DE EMPRESAS DE SOFTWARE NA REDE

Um velho chapa, Americo Oliveira
me enviou uma lista que vale ouro. Acho que podera' ser util
`a rapaziada. Dei so' um jeitinho no formato, que estava
meio enrolado de ler. Segura, negada...

Sites WWW para informacao/suporte:

Empresas de Hardware:

3k Associates (support for HP3000) http://www.3k.com/
Acorn Computers Ltd. http://www.acorn.co.uk/
Adaptec, Inc. http://www.adaptec.com/
Advanced RISC Machines, Inc. http://www.systemv.com/armltd/index.html
Amdahl Corporation http://www.amdahl.com/
Advanced Micro Devices, Inc. (AMD) http://www.amd.com/
Apple Computer, Inc. http://www.support.apple.com/
Aria WWW Home Page http://www.wi.leidenuniv.nl/aria/
ATI Technologies, Inc. http://www.atitech.ca/
BTG Incorporated http://www.btg.com/
BusLogic, Inc. http://www.buslogic.com/
Cisco Systems, Inc. http://www.cisco.com/
Compaq Computer Corporation http://www.compaq.com/
Cray Computer Corporation http://www.craycos.com/
Creative Labs, Inc. http://www.creaf.com/
Crystal Lake Multimedia, Inc. http://www.teleport.com:80/~crystal/
Cybernet Systems, Inc. http://www.cybernet.com/
Dell Computer Corporation http://www.dell.com/
Diamond Multimedia Systems, Inc. http://www.diamondmm.com/
DigiBoard http://www.digibd.com/
Digital Equipment Corporation http://www.digital.com/
Display Tech Multimedia, Inc. http://www.ccnet.com/~dtmi/
Ensoniq VFX (User Group) http://www.cs.colorado.edu/~mccreary/vfx/
Farallon Computing, Inc. http://www.farallon.com/
Gateway 2000 (User Group) http://www.mcs.com/~brooklyn/home.html
Global Village Communication, Inc. http://www.globalvillag.com/
HaL Computer Systems http://www.hal.com/
Hercules Computer Technology, Inc. http://www.dnai.com/~hercules/
Hewlett-Packard Company http://www.hp.com/
IBM Corporation http://www.ibm.com/
Intel Corporation http://www.intel.com/
Intergraph Corporation http://www.intergraph.com/
Media Vision, Inc. http://www.mediavis.com/
Micron (coming soon!!) http://www.micron.com/
MIPS Technologies, Inc. http://www.mips.com/
Motorola, Inc. http://www.mot.com/
Nanao USA Corporation http://www.traveller.com/nanao/
NCR Microelectronics http://www.ncr.com/
NEC USA, Inc. http://www.nec.com/
Network Computing Devices, Inc. http://www.ncd.com/
NVidia Corporation http://www.nvidia.com/
Olivetti North America http://www.isc-br.com/
Proteon, Inc. http://www.proteon.com/

QMS, Inc. http://www.qms.com/
Racal-Datacom, Inc. http://www.racal.com/
Radius, Inc. http://research.radius.com/
Rockwell International World Headquarters http://www.rockwell.com/
Samsung Semiconductor Corporation http://www.samsung.com/
Siemens-Nixdorf Information Systems http://www.sni.de/
Sceptre http://www.gus.com/emp/sceptre/sceptre.html
Silicon Graphics, Inc. http://www.sgi.com/
Sony (under construction) http://www.sony.com/
SPARC International, Inc. http://www.sparc.com/
Standard Microsystems Corporation (SMC) http://www.smc.com/
Sun Microsystems, Inc. http://www.sun.com/
Supra (coming soon!!) http://www.supra.com/
Synopsys, Inc. http://www.synopsys.com/
Tandem Computers, Inc. http://www.tandem.com/
Tatung Workstation R&D Group http://www.tatung.com/
Telebit Corporation http://www.telebit.com/
Thomas-Conrad Corporation http://www.tci.com/
Turtle Beach (Users Group)
http://www.cs.colorado.edu/~mccreary/tbeach/index.html
U.S. Robotics Corporation http://www.primenet.com/usr/
Western Digital Corporation http://www.wdc.com/
Wyse Technology http://www.wyse.com/wyse/
Xerox http://www.xerox.com/
Xircom http://www.organic.com/Ads/Xircom/
ZyXEL http://www.zyxel.com/

Empresas de Software:

Adobe Systems Incorporated http://www.adobe.com/
Apex Software Corporation http://www.apexsc.com/
Apple Computer, Inc. http://www.support.apple.com/
Berkeley Software Design, Inc. http://www.bsdi.com/
Berkeley Systems, Inc. http://proper.com:70/1/mac/sponsors/BerkeleySystems/
Booklink Technologies, Inc. http://www.booklink.com/
Bristol Technology, Inc. http://www.bristol.com/
Caere Corporation (coming soon!) http://www.caere.com/
Claris Corporation http://www.claris.com/
Compton's NewMedia, Inc. http://www.comptons.com/
Computer Associates http://www.adc.com/ingres/ca-info.html
Delrina Corporation http://www.delrina.com/
Fractal Design Corporation http://www.fractal.com/
FTP Software, Inc. http://www.ftp.com/
Gupta Corporation (under construction)
http://www.WJI.COM/mgupta/htmls/guphome.html
ID Software, Inc. (coming soon!!) http://www.idsoftware.com/
IBM Corporation http://www.ibm.com/
Insignia Solutions, Inc. http://www.insignia.com/
Intuit (under contruction) http://www.intuit.com/
Iona Technologies, Inc. http://www.iona.ie/
MathSoft, Inc. http://www.mathsoft.com/
MathWorks, Inc. http://www.mathworks.com/
McAfee Associates, Inc. http://www.mcafee.com/
Microsoft Corporation http://www.microsoft.com/
National Center for Supercomputing Applications http://www.ncsa.uiuc.edu/
NetManage, Inc. http://www.netmanage.com/
Netscape Communications Corporation http://mosaic.mcom.com/
NeXT Computer, Inc. http://www.next.com/
Novell, Inc. http://www.novell.com/
Oracle Corporation http://www.oracle.com/

Phoenix Technologies (BIOS) http://www.ptltd.com/
Quadralay Corporation http://www.quadralay.com/
Qualcomm Incorporated http://www.qualcomm.com/
Quarterdeck Office Systems, Inc. http://www.qdeck.com/
Responsive Software http://www.holonet.net/responsive/
SCO Open Systems Software http://www.sco.com/
Shiva Corporation http://www.shiva.com/
SoftQuad, Inc. http://www.sq.com/
SPRY, Inc. http://www.spry.com/
Spyglass, Inc. http://www.spyglass.com/
Storm Software, Inc. http://www.stormsoft.com/storm/
Symantec Corporation http://www.symantec.com/
Taligent, Inc. http://www.taligent.com/
Tidalwave Technologies, Inc. http://www.tidalwave.com/
Trusted Information Systems, Inc. http://www.tis.com/
VNP Software http://www.vnp.com/
Wall Data Incorporated http://www.walldata.com/
Wilson WindowWare, Inc. http://oneworld.wa.com/wilson/pages/index.html
WordPerfect http://www.wordperfect.com/
Ziff-Davis Publishing http://www.ziff.com/

Sites WWW de Suporte a Sistemas Operacionais:

Windows 95:

Microsoft Windows 95 Home Page
http://www.microsoft.com/pages/peropsys/win_news/chicago/wwwhtml/home/w95.htm

Windows NT:

Advanced Systems User Group http://128.150.146.76/ASUG.HTML
CSUSM Windows NT Archive Web Site
http://coyote.csusm.edu/cwis/winworld/nt.html
EMWAC Web Server Site http://emwac.ed.ac.uk/html/top.html
Rocky Mountain Windows NT User Group
http://budman.cmdl.noaa.gov/RMWNTUG/RMWNTUG.HTM
Stuttgart Windows NT User Group http://www.informatik.uni-
stuttgart.de/misc/nt/nt.html

OS/2:

Carnegie Mellon OS/2 WWW Home Page
http://www.club.cc.cmu.edu:8001/~jgrande/cmuos2.html
Cleveland OS/2 User Group Home Page
ftp://ftp.wariat.org/pub/users/cos2ug.html
The Internet Relay Chat OS/2 Homepage http://venus.ee.ndsu.nodak.edu/os2/
Mid-Atlantic OS/2 User Group Home Page
http://www.pinn.net/~reaper/maos2ug.html
The Munich OS/2 Archive http://www.leo.org/cgi-bin/leo-
dls/pub/comp/os/os2/00-index.html
North Suburban Chicago OS/2 User Group Home Page
http://www.mcs.com/~schmidtj/http/nscoug/home.html
OS/2 Stuff Worldwide Home Page http://tklab3.cs.uit.no/OS2/index.html
IBM OS/2 Warp Home Page http://www.austin.ibm.com/pspinfo/os2.html
The OS/2 WWW Homepage http://www.mit.edu:8001/activities/os2/os2world.html
OS/2 Information Page http://www.cen.uiuc.edu/~jt11635/os2/os2.html
OS/2 Internet Resources http://www.ccsf.caltech.edu/~kasturi/os2.html
OS/2 Power Home Page http://www.salford.ac.uk/os2power/os2power.html
The OS/2Web http://www.intac.com/nnjos2/os2web.html
UIUC OS/2 Home Page http://www.cen.uiuc.edu/~rs9678/raj.html

University of Texas OS/2 Home Page
http://deputy.law.utexas.edu/os2homepage.html
University of Warwick OS/2 Home Page http://www.warwick.ac.uk/~phueg/os2/
The Warp Pharmacy http://www.zeta.org.au/~jon/WarpPharmacy.html

Revistas de Computacao:

PC (DOS-Windows/ OS2/ Windows NT/ Windows 95):

CADalyst http://www.ideal.com/elprint/cadhome.html
Computer ResellerNews http://techweb.cmp.com/techweb/crn/current/default.html
Computer Retail Week http://techweb.cmp.com/techweb/crw/current/default.html
Computer Shopper http://www.shopper.ziff.com/~cshopper/
Datamation http://www.datamation.com/
Home PC http://techweb.cmp.com/techweb/hpc/current/default.html
InformationWeek http://techweb.cmp.com/techweb/iw/current/default.html
InfoWorld http://www.infoworld.com/
Microsoft Systems Journal http://www.mfi.com/msj/msjtop.html
Network Computing http://techweb.cmp.com/techweb/nc/current/default.html
PC Computing http://zcias3.ziff.com/~pccomp/
PC Magazine http://zcias3.ziff.com/~pcmag/
PC Week http://zcias3.ziff.com/~pcweek/
Windows Magazine http://www.wais.com:80/win/current/
Windows Rag Online Computer Magazine http://www.eskimo.com/~scrufcat/wr.html
Windows Sources http://zcias3.ziff.com/~wsources/

MAC:

InformationWeek http://techweb.cmp.com/techweb/iw/current/default.html
InfoWorld http://www.infoworld.com/
MacNet Journal http://www.netaxs.com/~aaron/hotlinks.html
MacUser http://www.macuser.ziff.com/~macuser/
MacWEEK http://www.ziff.com/~macweek/
PowerPC News http://power.globalnews.com/
ZiffNet/Mac http://zcias3.ziff.com/~zmac/

Outras:

Boardwatch Magazine (under contruction) http://www.boardwatch.com/
CommunicationsWeek http://techweb.cmp.com/techweb/cw/current/default.html
EE Times Interactive http://techweb.cmp.com/techweb/eet/current/default.html
HotWired Online Magazine http://www.wired.com/
InteractiveAge http://techweb.cmp.com/techweb/iaa/current/default.html
Inter@active Week http://www.interactive-week.ziff.com/~intweek/
Internet World http://www.mecklerweb.com/mags/iw/iwhome.htm
NetGuide http://techweb.cmp.com/techweb/ntg/current/default.html
NetSurfer Digest http://www.netsurf.com/nsd/index.html
VAR Business: Online Edition
http://techweb.cmp.com/techweb/vb/current/default.html

Repositorios para Suporte de Software / Hardware:

Empresas de Hardware:

3Com ftp://ftp.3com.com/
3k Associates(support for HP3000) ftp://ftp.3k.com/
Acorn Computers Ltd. ftp://ftp.acorn.co.uk/
Adaptec, Inc. ftp://ftp.adaptec.com/
Advanced Micro Devices, Inc. (AMD) ftp://ftp.amd.com/
American Megatrends, Inc. (AMI) ftp://american.megatrends.com

Apple Computer, Inc. ftp://ftp.apple.com/
Aria ftp://ftp.wi.leidenuniv.nl/pub/audio/aria/
Asante Technologies, Inc. ftp://ftp.asante.com/
ATI Technologies Inc. ftp://atitech.ca/
BusLogic, Inc. (coming soon!!!) ftp://buslogic.com/
Cabletron Systems ftp://134.141.197.25/
Cirrus Logic Corporation ftp://ftp.cirrus.com/
Compaq Computer Corporation ftp://ftp.compaq.com/
Cray Research ftp://ftp.cray.com/
Creative Labs, Inc. ftp://ftp.creaf.com/
Crystal Lake Multimedia, Inc. ftp://ftp.teleport.com/vendors/crystal/
Dell Computer Corporation ftp://ftp.dell.com/
Diamond Multimedia Systems, Inc. ftp://ftp.diamondmm.com/
Digital Equipment Corporation ftp://ftp.digital.com/
Farallon Computing, Inc. ftp://ftp.farallon.com/
Global Village Communication, Inc. ftp://ftp.globalvillag.com/
Hercules Computer Technology, Inc. ftp://ftp.netcom.com/pub/he/hercules
Hewlett-Packard Company ftp://ftp-boi.external.hp.com/
IBM PC Company (division) ftp://ftp.pcco.ibm.com/
Intel Corporation ftp://ftp.intel.com/
Intergraph Corporation ftp://ftp.intergraph.com/
Microcom ftp://ftp.microcom.com/
Micron (coming soon!!) ftp://micron.com/
MIPS Technologies, Inc. ftp://sgigate.sgi.com/
Motorola, Inc. ftp://bode.ee.ualberta.ca/pub/motorola/
NCR Microelectronics ftp://ftp.ncr.com/
NEC USA, Inc. ftp://ftp.nec.com/
Olivetti North America ftp://ftp.isc-br.com/
Panasonic Technologies, Inc. ftp://panasonic.com/
QMS, Inc. ftp://ftp.qms.com/
Samsung Semiconductor Corporation ftp://ftp.samsung.com/
Siemens-Nixdorf Information Systems ftp://ftp.mch.sni.de/
Silicon Graphics, Inc. ftp://ftp.sgi.com/
Standard Microsystems Corporation (SMC) ftp://ftp.smc.com/
Sony ftp://sony.com/
STB Systems, Inc. ftp://stb.com/
Sun Microsystems Binary3 Archive ftp://dalek.tiac.net/pub/sun3/
Supra ftp://ftp.supra.com/
Tadpole Technology, Inc. ftp://ftp.tadpole.com/
Texas Instruments ftp://ti.com/
U.S. Robotics Corporation ftp://ftp.usr.com/
Western Digital Corporation ftp://ftp.wdc.com/
Wyse Technology ftp://ftp.wyse.com/

Empresas de Software:

Adobe Systems Incorporated ftp://ftp.adobe.com/
Apple Computer, Inc. ftp://ftp.apple.com/
Asymetrix ftp://ftp.asymetrix.com/
Autodesk, Inc. ftp://ftp.autodesk.com/
Berkeley Software Design ftp://ftp.bsdi.com/
Booklink Technologies, Inc. ftp://ftp.booklink.com/
Borland ftp://ftp.borland.com/
Calera Recognition Systems ftp://calera.com/
Claris Corporation ftp://ftp.claris.com
Delrina Corporation ftp://ftp.delrina.com/
Fractal Design Corporation ftp://ftp.fractal.com/
FTP Software, Inc. ftp://ftp.ftp.com/
IBM Corporation ftp://software.watson.ibm.com/
Gupta Corporation ftp://wji.com/gupta/

ID Software, Inc. ftp://ftp.idsoftware.com/
Insignia Solutions, Inc. ftp://ftp.insignia.com/
MathWorks, Inc. ftp://ftp.mathworks.com/
McAfee Associates, Inc. ftp://ftp.mcafee.com/
Microsoft Corporation ftp://ftp.microsoft.com/
National Center for Supercomputing Applications ftp://ftp.ncsa.uiuc.edu/
NetManage, Inc. ftp://ftp.netmanage.com/
Netscape Communications Corporation ftp://ftp.mcom.com/
NeXT Computer, Inc. ftp://ftp.next.com/
Novell, Inc. ftp://ftp.novell.com/
Phoenix Technologies ftp://ftp.ptltd.com/=7F
Quadralay Corporation ftp://ftp.quadralay.com/
Qualcomm Incorporated ftp://ftp.qualcomm.com/
Quarterdeck Office Systems, Inc. ftp://ftp.qdeck.com/
SCO Open Systems Software ftp://ftp.sco.com/
Shiva Corporation ftp://shiva.com/
SoftQuad, Inc. ftp://ftp.sq.com/
SPRY, Inc. ftp://ftp.spry.com/
Spyglass, Inc. ftp://spyglass.com/
Symantec Corporation ftp://ftp.symantec.com/
Taligent, Inc. ftp://ftp.taligent.com/
Wilson WindowWare, Inc. ftp://oneworld.wa.com/wwwftp/wilson/
WordPerfect ftp://ftp.wordperfect.com/
Ziff-Davis Publishing ftp://ftp.zdbop.ziff.com/

HACKING AT THE END OF THE UNIVERSE

Rop Gonggrijp e Hanneke Vermeulen

(* Obs - texto nao traduzido integralmente. Publicado com permissao)

Tudo comecou em janeiro de 1993. Rop, a personificacao de Hack-Tic, e autor de mais um plano megalomano, fala de uma nova ideia sobre a qual estava pensando por algum tempo: um congresso de hackers ao ar livre. Em agosto de 1989, no Paradiso, um centro cultural de Amsterdan, organizaram juntos 'A Galactic Hacker Party'. Esta seria algo similar, mas ligeiramente diferente: em barracas e preferivelmente cortada do mundo civilizado.

Entao, tudo aconteceu. A organizacao comecou com coisas gerais: encontrar uma data, um terreno, oradores, e, pro-forma, um nome para o evento. Os autores deste artigo fizeram a toda a administracao. De acordo com uma tradicao antiga, saimos em uma 'viagem de negocios' ate' Bielefeld e Hamburgo para contar nossos planos a clubes alemaes de Hackers Foebud e Chaos Computer Club e a perdi-lhes uma mao.

No final de marco iniciamos nossa campanha de publicidade, a qual foi um grande exito. Nosso panfleto, que enviamos a 70 diarios e revistas diferentes, teve exatamente uma resposta. O comite 'Chamem Flevoland de Flevoland' esta horrorizado porque usamos a palavra 'Flevopolder' para indicar o lugar do congresso. Flevoland e' uma das provincias holandesas, e como esta' em um polder (terreno recuperado com ajuda dos diques), muita gente chama de Flevopolder.

Enquanto estavamos organizando, o tempo passa e a data do Congresso chega rapidamente. Todo tipo de coisas comecam a ficar dramaticamente reais. Cada vez mais nosso humor varia entre a esperanca (vai ser grandioso) e o medo (vai ser o pior fracasso de toda a historia..) Nao temos nem mais a minima ideia de quanta gente esperar (200? 1200?), tudo e'mais caro do que deveria ser, e nao temos administracao. Hanneke fixa desesperadamente seus pensamentos nos 500 hospedes imaginarios para os quais estamos organizando o congresso.

Rop nao pode dormir a noite, tendo visoes de tendas vazias, um terreno grande demais, e hackers desiludidos. Ja' aceitou a bancarrota de Hack-Tic e a sua propria desgraca.

Dois dias antes do comeco de "Hacking at the End of The Universe" comecamos com os preparativos no lugar. A equipe de rede ja havia conectado cabos, terminais, e modens em um lugar de prova por dois dias. Os voluntarios estao correndo freneticamente pelo terreno com mesas, computadores, barris de cerveja, telefones, pacotes de cabo Ethernet, barracas velhas do exercito, martelos, pregos, e aquele suor no rosto. No salao aparece um bar, uma rede de computadores, um stand onde se vendem coisas relacionadas com hackers. Por todo lado, cabos de eletricidade e cabos Ethernet estao lado a lado no chao. Um caso especial e' a conexao de seis linhas telefonicas extras. PTT Telecom, a empresa local de telefones, tem uma solucao perfeita para evitar conectar cabos extra. Com a ajuda de um multiplexor, podem nos dar oito linhas em dois cabos. Este metodo tem a desvantagem de nao se permitir o uso de fax e nao se podem usar comunicacoes por modem de alta velocidade pelas linhas. "Mas isto nao e' problema para festivais como estes, ne'?".

BLACKOUTS

Pintou um lance: a corrente. Os 22 KW, 220 volts que pudemos conseguir da companhia eletrica local estao completamente utilizados. Os monitores estao comecando a "sambar" e os micros fazem resets por vontade propria quando se liga a geladeira. Por hipotese, ja' tinhamos pensado nisso ha meses, por isso juntamos geradores para a energia extra. Mas, os geradores arrumados sao para trabalhos pesados.

Dai, de repente, no dia anterior ao comeco, no finalzinho da tarde, eles comecam a chegar: os visitantes. Estao vindo realmente. E parecem vir todos ao mesmo tempo. "O pessoal esta' chegando" grita Hanneke assustada, e de repente se da conta de que tudo isto e' real.

Mas o susto nao dura muito. Muita gente se oferece como voluntarios quando dizemos que precisamos de ajuda. Em muito pouco tempo temos equipes operando independentemente no bar e na recepcao. Gente que veio como visitantes perde a metade do programa sem se queixar, porcausa do trabalho. Varios parecem gostar de poder ajudar.

Tendas para tudo quanto e' lado.

Quando comeca o congresso, na quarta-feira dia 4 de agosto, o terreno esta lotado de tendas e todo mundo na maior. De repente, ate' o clima ta' demais, em meio a um verao extremamente umido e cinza. O discurso de abertura esta a cargo de Emmanuel Goldstein, editor da revista 2600 - Hacker Quaterly, dos EUA. Os 400 assentos da tenda grande estao ocupados. As laterais da tenda foram abertas e quem nao pode conseguir lugar esta' sentado na grama.

Esta tarde tem lugar o forum de discussoes 'networking para as massas' com aproximadamente 10 pessoas do mundo alternativo das redes no podio. Se trocam opinioes, e o que importa realmente nao e' a tecnica, mas principalmente o uso e a utilidade das redes de computadores.

Alem dos foros de discussao estao os workshops: Pengo, de Berlin, fala sobre os pontos fracos do sistema operacional VMS. Billsf e Rop dao um workshop no qual contam que tipo de mensagens interessantes de radio-amador da' para se captar com facilidade. David C., que tem uma companhia de computacao em Amsterdam, explica os principios do dinheiro digital anonimo. Foi desenvolvido um principio criptografico que permite substituir a "gaita" sem perder a privacidade daqueles que utilizam o sistema.

As pessoas que nao estao participando de um workshop se divertem, de todas as formas. No salao principal tem uns cinquenta micros em grandes filas sobre as mesas. Noite e dia tem caras surfando atraves do mundo pela Internet, apartir de Flevopolder. Volta e meia, alguem critica algum jogo ou copia algum programa. Quando uma alma solitaria abre sua colecao de fotos porno, a massa imediatamente esta olhando interessada sobre seu ombro. Quando esta' funcionando a rede dentro do salao, o campo e' conectado. Largos ramos de cabo coaxial entre as arvores e as vezes um repetidor em um saco de lixo, e voila': a primeira rede ethernet ao ar livre comeca a existir. As pessoas se sentam em grupos ao redor dos PCs como se fossem fogueiras de um acampamento.

Plano de emergencia

A tarefa de alimentar centenas de hackers famintos esta' nas maos de uma organizacao com o nome de 'Rampenplan'. Qualquer coisa assim como plano de emergencia ou desastre. Todos os dias os voluntarios preparam o cafe-da-manha, almoco e jantar em suas cozinhas portateis. Para alguns hackers essas comidas vegetarianas sao demasiado saudaveis, e todas as noites vemos quantidades de pizzas esfriando-se no salao principal, enquanto os entregadores estao buscando desesperadamente as donos dos pedidos.

A imprensa, que reagiu em marco com um silencio total ao anuncio deste congresso, vem em filas compactas em agosto, armados com microfones, maquinas fotograficas e equipe para filmar. Mas muitos visitantes nao querem encontrar suas caras nos diarios ou na televisao, por isso nao permitem 'as cameras filmar em todos os lugares. Os que querem permanecer incognitos podem comprar um par de oculos escuros numa pequena "hackshop". Alguns visitantes trasem suas proprias cameras de video e comecam, rindo-se, a contestar filmando os reporteres.

A imprensa tambem teve que pagar ingresso, como todos os fanaticos de computador mal-abastados. Nao ficaram muito contentes com isso. As equipes de filmagem (aos quais se permite entrar apenas com todo equipamento com apenas um ticket) se queixam de que dessa maneira apenas os jornalistas ricos podem ter a noticia enquanto descarregam cuidadosamente seu custoso equipamento de seus automoveis de luxo. Um jornalista ameaca escrever um artigo negativo sobre o congresso se tiver que pagar uma entrada, e realmente escreveu tal artigo.

(* Continua no proximo numero - presumindo-se que a revista continue ate' la' - Artigo tirado do numero 22/23 de novembro de 1993 da revista Hack-Tic *)

CRIME POR COMPUTADOR - 2a PARTE

:_Computers: Crime, Fraud, Waste Part 2
:_Written/Typed/Edited By: Lord Kalkin
:_Information Security

CRIMES, ABUSES, AND WASTE

A survey of goverment agancies identified techniques used in committing computer-related fraud and abuse. Few of these frauds and abuses involved destruction of computer equipment or

data. Only 3 percent of the frauds and 8 percents of the abuses involved willful damage or destruction of equipment, software or data. Most of the fraud and abuses cases involved information -- manipulating it, creating it, and using it.

THE FIVE MOST COMMON TECHNIQUES USED TO COMMIT COMPUTER-RELATED FRAUD AND ABUSE

Computer-Related Fraud

1. Entering unauthorized information
2. Manipulating authorized input information
3. Manipulating or improperly using information files and records
4. Creating unauthorized files and records
5. Overriding internal controls

Computer-Related Abuse

1. Stealing computer time, software, information, or equipment.
2. Entering unauthorized information
3. Creating unauthorized information fileas and records
4. Developing computer programs for nonwork purposes
5. Manipulating or improperly using computer processing

These techniques are often used in combination and are identified in Computer-Related Fraud and Abuse in Goverment Agencies, Department of Health and Human Services, Office of Inspector General, 1983.

Another way of looking at computer-related crime is to examine the types of crimes and abuses, and the methods used to commit them. These include:

"Data Diddling" - Probably the most common method used to commit computer crime because it does not require sophisticated technical knowledge and is relatively safe. Information is changed at the time of input to the computer or during output. For example, at input, documents may be forged, valid disks exchanged, and data falsified.

"Browsing" - Another common method of obtaining information which can lead to crime. Employees looking in others' files have discovered personal information about coworkers. Ways to gain access to computer files or alter them have been found in trash containers by persons looking for such information. Disks left on desks have been read, copied, and stolen. The very sophisticated browser may even be able to look for residual information left on the computer or on a storage media after the completion of a job.

"Trojan Horse" - This method assumes that no one will notice that a computer program was altered to include another function before it was ever used. A computer program with a valid, useful function is written to contain additional hidden functions that exploit the security features of the system.

"Trap Door" - This method relies on a hidden software or hardware mechanism that permits system protection methods to be circumvented. The mechanism is activated in some nonapperent manner. Sometimes the program is written so that a specific event, e.g., number of transactions processed or a certain calender date, will cause the unauthorized mechanism to function.

"Salami Technique" - So named because this technique relies on taking slices so small that the whole is not obviously affected. This technique is usually accomplished by altering a computer program. For example, benefit payments may be rounded down a few cents and these funds, which can be considerable in the aggregate, diverted to a fraudulent acount.

"Supperzapping" - Named after the program used in many computer centers which bypasses all system controls and is designed to be used in time of an emergency. Possession of this "master key" gives the holder opportunity to access, at any time, the computer and all of its information.

Examples of Compuer-Related crimes, abuses, and waste include:

- A payroll clerk, notified of a beneficiary's death, opened a bank account using the beneficiary's name and social security number. The beneficary was not removed from the computer eligibility lists, but a computer input form changed the address and the requested direct deposit of benefits to the payroll clerk's new bank acount.

- A major loss occurred with the diversion of the goverment equipment. Fictitious requisitions were prepared for routine ordering at a major purchasing centor. The rquisitions directed shipment of communications equipment to legitimate private corporations holding goverment contracts. Just prior to the delivery date, one of the conspirators would call the corporation to alert them of their "error" and arrange "proper" delivery of the equipment to the conspirators.

- Three data clerks, using a remote terminal, entered phony claims into the computer to recieve over $150,00 in benefits and then deleted records of these transactions to avoid being caught.

- Thefts of information commonly involve selling either personnel information, contract negotiation information (e.g., contract bids), and company proprietary information (e.g., product engineering information) for outside commercial use, or copying or using software programs for personal or personal business use.

CLUES

The following clues can indicate information security vulnerabilities:

1. Security policies and practices are nonexistant or not followed. No one is assigned responsibility for information security.
2. Passwords are posted nest to computer terminals, written in

obvoius places, shared with others, or appear on the computer screen when they are entered.
3. Remote terminals, microcomputers, and word processors are left on and unattended during work or nonwork hours. Data is displayed on unattended computer screens.
4. There are no restrictions on users of the information, or on the applications they can use. All users can access all information and use all trhe system functions.
5. There are no audit trails, and no logs are kept of who uses the computer for which operation.
6. Programming changes can be made without going through a review and approval process.
7. Documentation is nonexistant or inadequate to do any of the following: understand report definitions and calulations; modify programs; prepare data input; correct errors; evaluate system controls; and understand the data base itself -- its sources, records, layout, and data relationships.
8. Numerous attempts to log on are made with invalid passwords. In dialup systems -- those with telephone hookups -- hackers have programmed computers to do this "trial and error" guessing for them.
9. Input data is not subject to any verification or accuracy checks, or, when input data is checked:
    -- more data is rejected;
    -- more data adjustments are made to force reconciliation; or
    -- there is no record of rejected transactions.
10. There are excessive system crashes.
11. No reviews are made of computer information to determine the level of security needed.
12. Little attention is paid to information security. Even if an information policy exists, there is a prevailing view that it really is not needed.

INFORMATION SECURITY CONTROLS

1. Control access to both computer information and computer applications. Ensure only authorized users have access.

User Identification:

Require users to log on to the computer as a means of initial identification. To effectively control a microcomputer, it may be most cost-effective to use it as a single user systems. Typically, a microcomputer has no log-on procedures; authority to use the system is granted by simply turning on the computer.

User Authentication:

Use nontransferable passwords, avoiding traceable personal data, to authenticate the identity of the users. Establish password management protection controls, and educate users to common problems.

Other Controls:

Passwords are one type of identification -- something users knows. Two other types of identification which are effective are somthing that a user has -- such as a magnetic coded card -- or distinguished user characteristic -- such as a voice print

If the computer has a built in default password (a password that comes built into the computer software and overrides access controls) be sure it gets changed.

Consider having the computer programmed so that when the user log on, they are told the last time of its use and the number of invalid log-on attempts since then. This makes the user an important part of the audit trail.

Protect your Password

- Don't share your password -- with anyone
- Choose a password that is hard to guess
- Hint: Mix letters and numbers, or select a famous saying and select every fourth letter. Better yet, let the computer generate your password.
- Don't use a password that is your address, pet's name, nickname, spouse's name, telephone number or one that is obvious -- such as sequential numbers or letters.
- Use longer passwords because they are more secure; six to eight characters are realistic
- Be sure that your password is not visible on the computer screen when it is entered.
- Be sure that your password does not appear on printouts
- Do not tape passwords to desks, walls, or terminals. Commit yours to memory. <<---- Remember this!!!

Manage Passwords Carefully

- Change passwords periodically and on an irregular schedule
- Encrypt or otherwise protect from unauthorized access the computer stored password file.
- Assign password administration to the only most trusted officials.
- Do not use a common password for everyone in an area.
- Invalidate passwords when individuals leave the organization.
- Have individuals sign for their passwords.
- Establish and enforce password rules -- and be sure everyone knows them.

Authorization Procedures:

Develope authorization procedures that identify which users have access to which information and which applications -- and use appropriate controls.

Establish procedures to require management approval to use computer resources, gain authorization to specific information and applications, and recieve a password.

File Protection:

In addition to user identification and authorization procedures, develope procedures to restrict access to data files:

-- Use external file and internal file labels to identify the type of information contained and the required security levle;
-- Restrict access to related areas that contain data files such as off-site backup facilities, on-site libraries, and off-line files; and

-- Use software, hardware, and procedural controls to restrict
   access to on-line files to authorized users.

System Precaution:

-- Turn off idle terminals;
-- Lock rooms where terminals are located;
-- Position computer screens away from doorways, windows, and
   heavily tracked areas;
-- Install security equipment, such as devices that limit the
   number of unsuccessful log-on attempts or dial-back would be
   users who use telephones to access the computer;
-- Program the terminal to shut down after a specific time of
   non-use; and,
-- If feasible, shut down the system during nonbusiness hours.

CARTAS - NEWS:

Sobre a "famosa" ideia de reunir a rataiada para um bate papo aqui em Sampa, nada rolou ainda. Mas consegui descobrir que a mocada de algumas BBSes tipo a Mandic e a Persocom parece que ja' tem um grupo de ratos que combinam de se reunir em um bar na av. Reboucas. Isso foi uma pos-graduanda que me falou. Tenho minhas duvidas se e' verdade, porque esse tipo de coisa teria divulgacao num jornal, mas em se tratando de iniciativa privada, tudo e' possivel. O proximo BE deve sair em duas semanas, e se eu descobrir qualquer coisa ate' la', informo. Tenho que confessar minha total incompetencia para descolar um local decente, uma das razoes pela qual nao chamei a rapeize. A USP, para quem nao sabe, atualmente fecha aos fins-de-semana, inviabilizando o que seria o melhor lugar de encontro, ja' que conto com ajuda p. reservar sala p. o dito.

Esta aqui e' para quem acha que so' software pirata transmite virus.

Newsgroups: comp.virus
Subject: "Microsoft ships Form" (PC)
Date: 1 Mar 1995 18:14:24 -0000
Lines: 41
Original-Sender: news@Lehigh.EDU
Approved: news@netnews.cc.lehigh.edu
Distribution: world
Message-Id: <0007.9503011339.AA01815@bull-run.assist.mil>
Nntp-Posting-Host: fidoii.cc.lehigh.edu
Status: R

You may be interested to hear that the top story in the UK at the moment is that according to reports in the computer industry press, Microsoft have accidentally distributed the Form virus.

According to the story on the front page of Computer Weekly magazine (23 Feb 95) They accidentally distributed Form to 200 of the UK's leading software developers. This happened last week in London at a Windows 95 Internationalisation seminar, when developers were handed a floppy disk of sample code and document files.

The virus was spotted by a delegate who reported it to Microsoft, prompting a full apology from the company. Microsoft wrote to developers warning of the defect, recommending that they scan their disks with anti-virus software.

A Microsoft spokesman blamed its disk supplier for the virus. "It is in [the supplier's] contract to virus-check the disks they supply to us", he said, admitting that the problem was "highly embarrassing".

Microsoft claims it is normally vigilant in the testing of disks it hands out to users and developers, but that it ran out of time in the duplication of its seminar disks.

Regards
Graham
\- ---

Graham Cluley   [gcluley@sands.co.uk]
Senior Technology Consultant,   S&S International PLC, Alton House,
Dr Solomon's Anti-Virus Toolkit   Gatehouse Way, Aylesbury, Bucks, UK
S&S International PLC   +44 (0)1296 318700
,,
In the States contact: S&S Software International, Inc,
27660 Marguerite Parkway #C-250, Mission Viejo, CA 92692, USA
Tel: 714 470 0048 Fax: 714 470 0018 [72714.2252@compuserve.com]

===

Para comentar essa outra carta, antes vou ter que mencionar o incidente anterior.

PIRATA ELETRONICO INVADE ARQUIVOS DA USP

Condensado da materia do
Estado de Sao Paulo - 23-2-95 - Neide Maria Silva

Sao Carlos - A onda dos hackers, os piratas eletronicos que se divertem descobrindo senhas que dao acesso a arquivos de computacao, chegou semana passada a Universidade de Sao Paulo. O primeiro departamente a ter parte de seus arquivos apagadosfoi a Engenharia Eletrica, na terca-feira. No dia seguinte, o ataque foi na Fisica, que perdeu informacoes armazenadas em tres discos e ficou com uma importante estacao de trabalho parada seis horas. Audacioso, o hacker entrou tambem com sucesso nos sistemas do Departamento de Matematica, na quinta-feira.

A acao foi considerada como "uma brincadeira maldosa", ja' que o hacker nao teve nenhum proveito pratico com o ataque. O assunto foi mantido em sigilo para evitar atrair a atencao de outros genios ciberneticos. Segundo o professor Jan Slacts, responsavel pelo servico de informatica do Departamento de Fisica, a invasao comecou por volta das tres horas da madrugada e o hacker chegou a pedir aos usuarios que estavam no sistema para que avisassem o FANTASTICO sobre o que ele estava fazendo.

EFEITOS COLATERAIS NO BARATA ELETRICA

Na terca-feira, a coluna Netvox, do Jornal FOLHA DE SAO PAULO, comentou a existencia do Barata Eletrica, como o primeiro Hacker E-Zine Brasileiro. Isso, logo apos o "break-in" no computador da USP em Sao Carlos.

Todo computador ligado a Internet tem a sua equipe de Sysops ou "Super-Users", encarregados de fazer a manutencao e controlar o acesso a maquina. O encarregado da maquina onde eu tinha a conta que foi anunciada no jornal congelou o acesso a minha conta, ate' que eu aparecesse para explicar o quais eram minhas intencoes. Tive que explicar que minha preocupacao era sobre hacking e nao cracking (vandalismo eletronico).
Mesmo assim, como havia uma especie de caca as bruxas, ele me pediu para arrumar outra forma de manter minha lista eletronica. No meu local de trabalho, tambem me falaram quase a mesma coisa. "O problema sao as macas podres", Derneval.

A CARTA QUE RECEBI, NUM BELO DIA, NA MINHA CONTA

>From tunel@univap.br Mon Apr 17 13:01:03 1995
>Date: Sun, 9 Apr 95 16:39:13-030
>From: Tunel do tempo
>To: ??????????????????
>Subject: TRUE H4CK

E ai Denerval, como anda o H4CK? Pena que a B4R4T4 3L3TR1C4 sejam muito fraca, precisa um pouco mais de sal e um pouco menos de V1RUS.:)
Nos somos conhecidos como C.R.A.Y (Computers Rats Against Ydiots) somos os responsaveis por uma serie de ataques, inclusive o qual voce foi responsabilizado ai na USP. :o
Quanto ao SUMMERCON seria uma boa uma vez que a classe H4CK e muito desunida. Preste atencao a TV e voce podera nos ver agindo. :o
Mande lembrancas para o L4M3R do Arnaldo (vulgo ARNIE no IRC) da QuimicaMolecular, e avise para ele que nao se deve rodar SN1FF3RS num maquina como a C4T.:)
Que tal a gente comecar a invadir os .COM.BR. :) Ou criar um canal no IRC tipo #HBRAZIL, toda quarta-feira a partir das 20:00. Avise os seus amigos confiaveis, porque o H4CK e coisa seria pra nos. :)

JOIN C.R.A.Y (Satan Inside)

REPLY > /DEV/NULL

P.S.: Ao Sr. Gomide, "REPENT THE END IS NEAR ... " MAYBE TO FAR AWAY :)
Ao Sr. Becherini, "NOS JA CONVERSAMOS POR TELEFONE"
Ao Sr. Cansian, "ACREDITO QUE A REAVALICAO NAO FUNCIONE" :)
Ao Sr. Dan Farmer, "AGRADECO POR TUDO"
Ao Sr. Papai e Mamae, "VOCES SAO MAXIMO!"

SPONSORED BY: SUN MICROSYSTEMS
EMBRATEL
RENPAC
TELESP E' COELHINHO
RNP
E OBVIAMENTE A FAPESP.

INTEL

==========
Resposta de um amigo meu a ideia

Subject: Re: TRUE H*** (fwd)

Hmm... Interessante... Sera' que e' verdade ou so' sao LAMMERS??? Em todo caso, volto a sugerir a opcao do talker. Seria um talker restrito, e as contas deveriam ser criadas por mim. Se voce achar uma boa...

Abracos,

?????? ??????

==========

Minha resposta e' que eu nao tenho uma proposta de Vandalismo Eletronico, ou ficar exibindo conhecimentos para a midia. Acho a vida muito curta.

Colocar um monte de caras viciados em micro numa sala, para trocar historias e dicas sobre problemas pelos quais todo mundo passa. E passando adiante as experiencias. Se a conversa esbarrar em "Computer Underground", tudo bem. Tem muita gente por ai que aprende Carate, Judo, ate' Ninjutsu, mas nao sai matando gente. Existem grupos de gentes apaixonados por romances de espionagem, assaltos,etc, que nao saem por ai nem vasculhando a vida das pessoas nem assaltando bancos. Ser Hacker nao tem nada a ver com vandalismo eletronico, e e' com esta visao que faco o meu e-zine.

BIBLIOGRAFIA:
==========

The Digital Personna and its Application to Data Surveillance - Roger Clarke - The Information Society

Manual do Espiao

The Code-Breakers - David Kahn

Revista Super-Interessante - janeiro de 94

N.I.A - Network Information Access nr 4

PGP versao 2.6i - arquivos pgpdoc1.txt pgpdoc2.txt

Hack-Tic - novembro de 1993

Virus Report nr 18

From tunel@univap.br Mon Apr 17 13:01:03 1995
Date: Sun, 9 Apr 95 16:39:13-030
From: Tunel do tempo
To: ?????@???????????
Subject: TRUE H4CK

E ai Denerval, como anda o H4CK? Pena que a B4R4T4 3L3TR1C4 sejam muito fraca, precisa um pouco mais de sal e um pouco menos de V1RUS.:)

Nos somos conhecidos como C.R.A.Y (Computers Rats Against Ydiots) somos os responsaveis por uma serie de ataques, inclusive o qual voce foi responsabilizado ai na USP. :o
Quanto ao SUMMERCON seria uma boa uma vez que a classe H4CK e muito desunida. Preste atencao a TV e voce podera nos ver agindo. :o

Mande lembrancas para o L4M3R do Arnaldo (vulgo ARNIE no IRC) da QuimicaMolecular, e avise para ele que nao se deve rodar SN1FF3RS num maquina como a C4T.:)

Que tal a gente comecar a invadir os .COM.BR. :) Ou criar um canal no IRC tipo #HBRAZIL, toda quarta-feira a partir das 20:00. Avise os seus amigos confiaveis, porque o H4CK e coisa seria pra nos. :)

JOIN C.R.A.Y (Satan Inside)

REPLY > /DEV/NULL

P.S.: Ao Sr. Gomide, "REPENT THE END IS NEAR ... " MAYBE TO FAR AWAY :)
Ao Sr. Becherini, "NOS JA CONVERSAMOS POR TELEFONE"
Ao Sr. Cansian, "ACREDITO QUE A REAVALICAO NAO FUNCIONE" :)
Ao Sr. Dan Farmer, "AGRADECO POR TUDO"
Ao Sr. Papai e Mamae, "VOCES SAO MAXIMO!"

SPONSORED BY: SUN MICROSYSTEMS
EMBRATEL
RENPAC
TELESP E' COELHINHO
RNP
E OBVIAMENTE A FAPESP.

INTEL

==========
Resposta de um amigo meu a ideia

Subject: Re: TRUE H*** (fwd)

Hmm... Interessante... Sera' que e' verdade ou so' sao LAMMERS??? Em todo caso, volto a sugerir a opcao do talker. Seria um talker restrito, e as contas deveriam ser criadas por mim. Se voce achar uma boa...

Abracos,

?????? ??????

==========

Minha resposta e' que eu nao tenho uma proposta de Vandalismo Eletronico, ou ficar exibindo conhecimentos para a midia. Acho a vida muito curta.

Colocar um monte de caras viciados em micro numa sala, para trocar historias e dicas sobre problemas pelos quais todo mundo passa. E passando adiante as experiencias. Se a conversa esbarrar em "Computer Underground", tudo bem. Tem muita gente por ai que aprende Carate, Judo, ate' Ninjutsu, mas nao sai matando gente. Existem grupos de gentes apaixonados por romances de espionagem, assaltos,etc, que nao saem por ai nem vasculhando a vida das pessoas nem assaltando bancos. Ser Hacker nao tem nada a ver com vandalismo eletronico, e e' com esta visao que faco o meu e-zine.

BIBLIOGRAFIA:
==========

The Digital Personna and its Application to Data Surveillance - Roger Clarke - The Information Society

Manual do Espiao

The Code-Breakers - David Kahn

Revista Super-Interessante - janeiro de 94

N.I.A - Network Information Access nr 4

PGP versao 2.6i - arquivos pgpdoc1.txt pgpdoc2.txt

Hack-Tic - novembro de 1993

Virus Report nr 18