

2008 - Lessons Learned

Bruno Morisson



Agenda

RFID Mifare Crypto-1 Cracked
Debian OpenSSL "Patch"
Kaminsky DNS Vulnerability
Outras Vulnerabilidades
Futurologia

RFID MiFare Crypto-1 Cracked

RFID MiFare Crypto-1 Cracked

- Chip RFID fabricados pela NXP
- Usado em diversas aplicações (controle de acessos, autenticação, etc)
- Cartão Contactless mais utilizado no mundo
- O fabricante diz que tem "advanced security levels"
- Algoritmo proprietário (chave de 48 bits)

RFID MiFare Crypto-1 Cracked

Dec. 2007 - Karsten Nohl e Henry Plotz -
Reverse Engineering do Hardware.

Mar. 2008 - Radboud University Nijmegen
(Holanda) - Demonstraram acesso a um
edifício.

RFID MiFare Crypto-1 Cracked

Impacto:

- Passes Sociais - Holanda, EUA, UK, China, Brasil
- Controlo de Acessos

“1 billion of MiFare Classic chips are used worldwide, including in many governmental security systems”

“key recovery in twelve seconds”

RFID MiFare Crypto-1 Cracked

“um criptosistema deve ser seguro mesmo que tudo sobre o sistema, excepto a chave, seja de conhecimento público”

Auguste Kerckhoffs, 1883

RFID MiFare Crypto-1 Cracked

- Algoritmos fechados são “perigosos”
“Consideration should be given to the independent review of the algorithm” - RHUL Report
- Tradeoff Segurança/Preço/Capacidade Processamento

Debian OpenSSL "patch"

Debian OpenSSL "patch" CVE-2008-0960

- 13 Maio 2008 - Debian publica um advisory anunciando um problema no RNG nos seus packages de OpenSSL

Debian OpenSSL "patch" CVE-2008-0960

- Debian GNU/Linux:
 - Distribuição baseada no Kernel Linux
 - Gestão de Packages próprios
 - Branches: Unstable / Stable

Debian OpenSSL "patch" CVE-2008-0960

- OpenSSL:
 - Biblioteca "standard" para operações criptográficas
 - FIPS 140-2
 - Utilizada em software OSS e proprietário

Debian OpenSSL "patch" CVE-2008-0960

- RNG - Random Number Generator
- PRNG - Pseudo-Random Number Generator
- Entropia - Mede a imprevisibilidade dos dados. "More is better". Numa sequência aleatória, idealmente a entropia é igual ao tamanho da sequência.

Debian OpenSSL "patch" CVE-2008-0960

- RNG da OpenSSL da Debian era...



...previsível...

Debian OpenSSL "patch" CVE-2008-0960

... desde 17 Set 2006!

```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
             // guaranteed to be random.  
}
```

DEBIAN

GUARANTEED ENTROPY.

Debian OpenSSL "patch" CVE-2008-0960

- Alteração feita devido a 2 ferramentas de validação de código (Valgrind e Purify) se queixarem
- A Debian contactou (via mailing list) a equipa do OpenSSL
- Ninguém achou má ideia comentar o código...

Debian OpenSSL "patch" CVE-2008-0960

version 140, Tue May 2 16:25:19 2006 UTC

Line 271

```
else
    MD_Update(&m,&(state[st_idx]),j);
```

```
MD_Update(&m,buf,j);
```

```
MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
MD_Final(&m,local_md);
md_c[1]++;
```

Line 465

```
MD_Update(&m,local_md,MD_DIGEST_LENGTH);
MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
```

```
#ifndef PURIFY
```

```
MD_Update(&m,buf,j); /* purify complains */
```

```
#endif
```

```
k=(st_idx+MD_DIGEST_LENGTH/2)-st_num;
if (k > 0)
```

Debian OpenSSL "patch" CVE-2008-0960

version 141, Tue May 2 16:34:53 2006 UTC

Line 271

```
else
    MD_Update(&m,&(state[st_idx]),j);
```

```
/*
```

```
 * Don't add uninitialised data.
```

```
    MD_Update(&m,buf,j);
```

```
*/
```

```
    MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
```

```
    MD_Final(&m,local_md);
```

```
    md_c[1]++;
```

Line 468

```
    MD_Update(&m,local_md,MD_DIGEST_LENGTH);
```

```
    MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
```

```
#ifndef PURIFY
```

```
/*
```

```
 * Don't add uninitialised data.
```

```
    MD_Update(&m,buf,j); /* purify complains */
```

```
*/
```

```
#endif
```

```
    k=(st_idx+MD_DIGEST_LENGTH/2)-st_num;
```

```
    if (k > 0)
```

Debian OpenSSL "patch" CVE-2008-0960

- Em vez de usar dados aleatórios, o OpenSSL passou a usar um valor entre 1 e 32768 (PID)
- "Q: How long did it take to generate these keys?
A: I used 31 Xeon cores clocked at 2.33Ghz. It took two hours to generate the 1024-bit DSA and 2048-bit RSA keys for x86. The 4096-bit RSA keys took about 6 hours to generate." - HD Moore (MetaSploit)

Debian OpenSSL "patch" CVE-2008-0960

- Impacto:
 - "Affected keys include SSH keys, OpenVPN keys, DNSSEC keys, and key material for use in X.509 certificates and session keys used in SSL/TLS connections."
 - Todas as chaves SSL e SSH geradas em sistemas baseados em Debian entre Set 2006 e Maio 2008 (debian/*ubuntu/etc)
 - As chaves geradas em debian/ubuntus e usadas noutros sistemas...

Debian OpenSSL "patch" CVE-2008-0960

- Alterar código complexo sem o compreender profundamente, é arriscado
- Mesmo quem o devia compreender, sem contexto pode tomar decisões erradas
- Nem sempre "Many Eyes Make All Bugs Shallow"
- O patch nunca foi submetido upstream...

Debian OpenSSL "patch" CVE-2008-0960

Kaminsky DNS Vulnerability

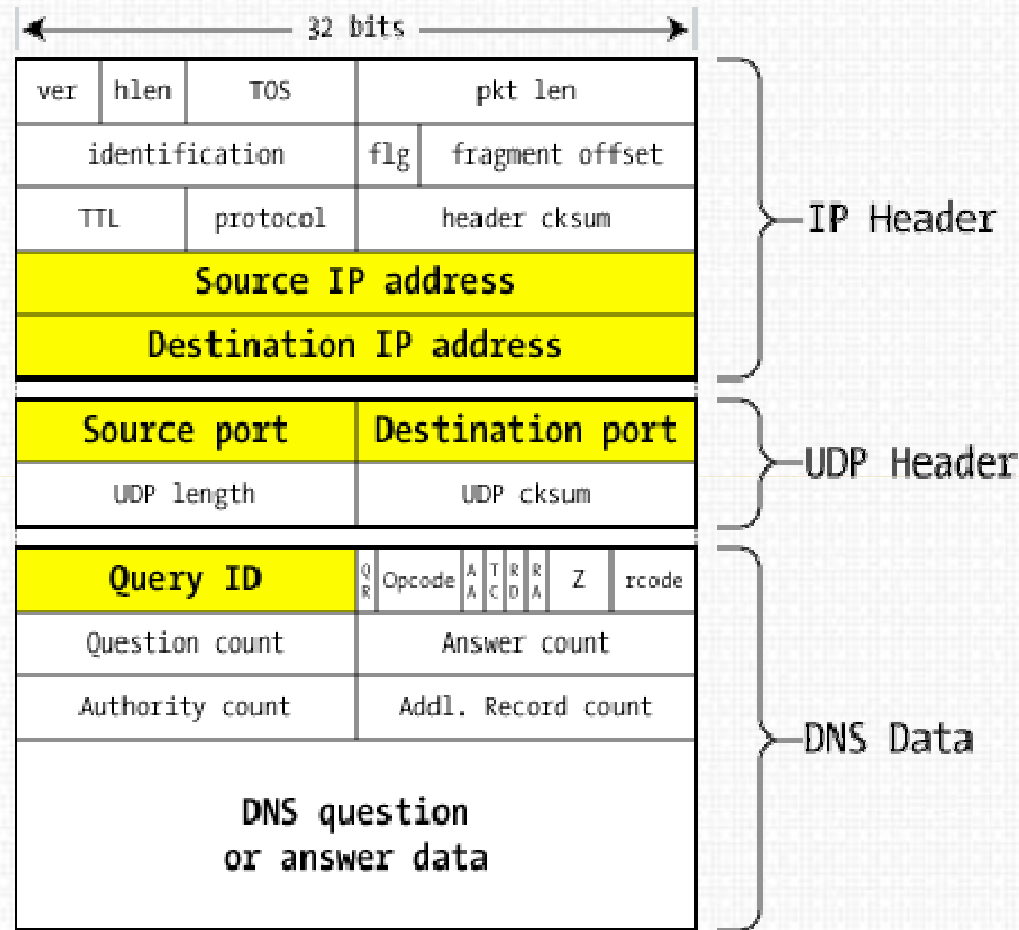
Kaminsky DNS Vulnerability CVE-2008-1447

- 8 Julho 2008 - CERT Advisory:
 - Multiple DNS implementations vulnerable to cache poisoning
- Detalhes não divulgados
- Dan Kaminsty publicaria os detalhes durante a BlackHat Briefings 2008 (LV)

Kaminsky DNS Vulnerability CVE-2008-1447

- Insufficient transaction ID space:
 - TXID - 16bits
- Fixed source port for generating queries
 - Previsível qual o Source Port, fazendo apenas uma query

Kaminsky DNS Vulnerability CVE-2008-1447



DNS packet on the wire

Kaminsky DNS Vulnerability CVE-2008-1447

- Crash Course on DNS:
 - User: "Quem tem o endereço www.xpto.pt ?"
 - Servidor ISP procura qual o servidor que tem o domínio xpto.pt (autoritário)
 - Servidor ISP pergunta "qual o endereço www.xpto.pt?"
 - Servidor Autoritário responde "1.1.1.1"
 - Servidor ISP responde "1.1.1.1"

Kaminsky DNS Vulnerability CVE-2008-1447

- Crash Course on DNS II (ataque):
 - Atacante: "Quem tem o endereço www.xpto.pt?"
 - Servidor ISP procura qual o servidor que tem o domínio xpto.pt (autoritário)
 - Servidor ISP pergunta "qual o endereço www.xpto.pt?"
 - **Atacante responde "2.2.2.2"**
 - Servidor Autoritário responde "1.1.1.1"

Kaminsky DNS Vulnerability CVE-2008-1447

- Quem responder primeiro, ganha a corrida!
 - Atacante: 1 / 65536
- Problemas:
 - Adivinhar o TXID
 - Quem ganhar a corrida fica na "cache" durante um tempo pré-definido "TTL"

Kaminsky DNS Vulnerability CVE-2008-1447

- Qual a novidade ?
 - Dan Kaminsky descobriu que é possível sobrepor a cache!
 - Problema: Glue Records / Bailwick
 - Glue Records: Permitem que o servidor autoritário de determinado domínio adicione informação à resposta.
 - ex: `www.xpto.pt` in a `6.6.6.6`

Kaminsky DNS Vulnerability CVE-2008-1447

- Como atacar ?
 - Perguntar por "1.xpto.pt", "2.xpto.pt", "3.xpto.pt", "aaaaa.xpto.pt" (...) e responder
 - Parte do problema do TTL resolvido - Aumenta a probabilidade de sucesso
 - Adicionar um Glue Record na resposta "www.xpto.pt in a 6.6.6.6"
 - Problema do TTL resolvido: o servidor vai sobrepor o registo anterior, independentemente do TTL original

Kaminsky DNS Vulnerability CVE-2008-1447

- A maioria das implementações eram vulneráveis:
 - Microsoft DNS
 - BIND
- Mas algumas não:
 - DjbdNS
 - PowerDNS

Kaminsky DNS Vulnerability CVE-2008-1447

- Source Port Randomization:
 - Daniel J. Bernstein
(Qmail/DjbDNS/DaemonTools/...)
- "DJB was Right" - Dan Kaminsky
 - Desde Julho 2001

Kaminsky DNS Vulnerability CVE-2008-1447

- Julho de 2001:

“Wrong. Randomizing the port number makes a huge difference in the cost of a forgery for blind attackers---i.e., most attackers on the Internet.”

	Nº Tentativas
nada	1
BIND (TX ID)	65536
DjbDNS (TX ID*Port)	4227727360

Kaminsky DNS Vulnerability CVE-2008-1447

- Torna o ataque impraticável:
 - É possível, mas o tráfego necessário é detectável
- Outras soluções passam por fazer um upgrade a todo o sistema de DNS (DNSSEC)

Kaminsky DNS Vulnerability CVE-2008-1447

- Impacto:
 - 85% dos servidores DNS vulneráveis
 - Tudo depende do DNS
 - Mail (MX)
 - Web
 - VPN
 - NTP
 - ...

Kaminsky DNS Vulnerability CVE-2008-1447

- Quebra de Confidencialidade e Integridade
 - Intercepção de comunicações
 - Man-in-the-middle

Kaminsky DNS Vulnerability CVE-2008-1447

- Bom design (paranoia?) de software (DJB)
- Estamos dependentes de tecnologias desenvolvidas há > 20 anos
 - Segurança não era prioridade nem preocupação

Outras Vulnerabilidades

- BGP
 - Demonstração de como é possível interceptar tráfego IP
 - Já conhecido, nunca demonstrado publicamente
- SNMPv3
 - Validação de HMACs, com 1 byte (256)

Outras Vulnerabilidades

- ColdBoot
 - Possível recuperar conteúdo da RAM mesmo após o computador ter sido desligado
- ClickJacking
 - Exploração da possibilidade de usar vários conteúdos/componentes numa página web, para “manipular” o utilizador

Futurologia

- Browser security:
 - O browser é cada vez mais a nossa "casa"
 - Extremamente complexas as interacções entre componentes, plugins, sistema operativo, outras aplicações
 - Mesmo quando é bem pensado, falha (Google Chrome)

Futurologia

- Protocolos "arcaicos"
 - Tecnologias com 20 anos, inseguras
 - Outras com quase tantos (BGP-4: RFC 1171 1995... update em 2006! - RFC 4271)
 - Dificuldade de actualizar

Q&A

www.onicommunications.pt

bruno.morisson@oni.pt



youuniversal business solutions



onicommunications

youniversal business solutions