Slutrapport för Better-than-nothing security

Michael Cardell Widerkrantz
mc@hack.org
2012-11-06

1. Inledning

Projektet *Better-than-nothing security* har fått stöd av .SE-stiftelsen. Detta är den publika versionen av slutrapporten från projektet.

2. Mål och syfte

Projektet har haft som mål att implementera Better-than-nothing security (BTNS), IPsec med anonyma nycklar [1] [2].

Syftet med projektet har varit att visa på att BTNS överhuvudtaget *kan* implementeras och att ge tillgång till en fri BTNS-implementation för experiment och framtida standardisering.

3. Projektbeskrivning

Projektet har framför allt bestått av research och programutveckling. Till en början skapades en mer detaljerad att göra-lista, därefter studerades olika fria implementationer av nyckelförhandlingsprotokollet IKEv2 [3]. En implementation valdes, OpenBSD:s *iked*. Därefter implementerades BTNS-stöd i *iked* efter specifikationerna.

Mycket tid har lagts på kommunikation: Skrivandet av en serie bloginlägg,[1] deltagande i brevlistor, direkt korrespondens med andra utvecklare och forskare och skrivande av dokumentation om hur hur man använder den förändrade *iked*.

4. Leverabler

Samtliga leverabler finns tillgängliga på projektets websida.[2] Projektet har framställt:

- En serie patchar till *iked*, inklusive manualförändringar: En patch för att stödja RSA-nycklar av typ 11, se RFC 5996, Section 3.6[3], som är ett villkor för BTNS, och en patch för att stödja BTNS per se.
- Ett program, *rsafap*, för att beräkna fingeravtryck av RSA-nycklar på samma sätt som patchen till *iked* gör.
- Ett dokument av HOWTO-typ som beskriver hur man sätter upp systemet.

5. Resultat

Projektet har framgångsrikt visat med körande kod att det går att implementera BTNS. Minst en av patcharna framställda i projektet (stöd för RSA-nycklar) kan komma att accepterats med vissa förändringar av OpenBSD-projektet.

---

[1] Se *http://hack.org/mc/blog/*

[2] *http://hack.org/mc/projects/btns/*

6. Utvärdering och analys

6.1. Utvärdering av resultat

Projektet har uppnått allt som åtagits enligt avtalets bilaga 2. På grund av sjukdom blev projektet omkring tre veckor försenat.

Då *iked* inte stöder Transport Mode stöds heller inte detta av BTNS-implementationen. Det är inte helt klart från specifikationen huruvida det är ett krav att köra Transport Mode eller om Tunnel Mode accepteras. Det finns emellertid välkänd kritik mot att komplicera IPsec med skillnaden mellan Transport och Tunnel Mode [4]. I praktiken fungerar det alldeles utmärkt att köra Tunnel Mode mellan två ändnoder både med och utan BTNS.

6.2. Förslag på förbättringar

En tänkbar förbättring är att implementation av Transport Mode i *iked*, kanske enbart för för BTNS. För att gå vidare krävs diskussion inom standardorgan och mer testning.

I implementationen som finns idag används eventuella BTNS wildcards, speciella fingeravtryck som matchar *alla* noder som vill koppla upp, i *alla* policies som tillåter BTNS. Det är inte säkert att det är önskvärt. Kanske vill man specifikt tillåta inte bara BTNS utan också ”BTNS med wildcard” per policy. För att gå vidare krävs rapporter från användare.

En begränsning i OpenBSD och/eller *iked* gör att man för nuvarande inte kan ha IPsec-policies i kärnan där man samtidigt är initierande i IKE-dialogen och har motparter som är definierade som nätverk. I stället måste man ange sin motpart exakt om man vill initiera IKE-förhandlingen. Förhandlingen görs också direkt vid start av *iked* och inte när det kommer trafik som matchar policyn.

För att BTNS skall komma till sin rätt i större skala vore det önskvärt att kunna uttrycka även policies med nätverk som motpart även om noden skall vara den initierande i IKE-dialogen.

7. Framtida arbeten

Idag är OpenBSD:s *iked* den enda IKE-servern som stöder någon form av BTNS. Det känns naturligt att fortsätta projektet genom att porta *iked* till andra plattformar, i första hand FreeBSD och Linux. Portningen skulle troligen också ge andra fördelar, till exempel med hjälp av annan IPsec-stack kunna ha policies med aktiv IKE-förhandling där motparten i policyn är ett nätverk och inte en exakt adress.

I ett tidigare .SE-projekt, *Opportunistisk kryptering på IP-nivå*, skapades en serie patchar till en IKEv1-server, *racoon*, och ett antal Perl-script för att utnyttja DNS för nyckeldistribution. Det vore önskvärt att anpassa Perl-scripten att i stället använda IKEv2. Närmast till hands ligger att helt enkelt anpassa dem till *iked*.

Referenser

1. M. Richardson, N. Williams, “Better-Than-Nothing Security: An Unauthenticated Mode of IPsec,” RFC 5386 (November 2008).
2. J. Touch, D. Black, Y. Wang, “Problem and Applicability Statement for Better-Than-Nothing Security (BTNS),” RFC 5387 (November 2008).
3. C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, “Internet Key Exchange Protocol Version 2 (IKEv2),” RFC 5996 (September 2010).
4. Niels Ferguson, Bruce Schneier, *A Cryptographic Evaluation of IPsec* (1999). http://www.schneier.com/paper-ipsec.pdf.