

Re: Code breakers beat security scheme of car locks, gas pumps

Source: <http://sci.tech-archive.net/Archive/sci.physics/2005-02/2579.html>

From: Uncle Al (UncleAl0_at_hate.spam.net)

Date: 02/06/05

Date: Sat, 05 Feb 2005 18:33:29 -0800

Ian Stirling wrote:

>

> Uncle Al <UncleAl0@hate.spam.net> wrote:

> > Ian Stirling wrote:

> > >

> > > Uncle Al <UncleAl0@hate.spam.net> wrote:

> > > > Ian Stirling wrote:

> > > > <sniop>

> > > > > However, it depends on the resources of the attacker.

> > > > > I'm not very worried if it takes ten thousand PCs a year to crack one car.

> > > >

> > > > > Once the algorithm is broken you eavesdrop on cantu or respondu.

> > > >

> > > > Which doesn't matter.

> > > > If it costs you \$1M to crack a car code, then unless you've got a very

> > > > special car, it's not a problem.

> > > >

> > > > (However, I note that it takes about 20 PC-weeks to crack a key, with

> > > > non-special hardware)

> > > > Or not that large an investment.

> >

> > > If you run in Linux, 1.4X faster than in Windows. If you run in AMD,

> > > then 1.4X faster than in Intel. My new iron, an Athlon 55FX

>

> Unless you know the algorithm, you can't generalise.

> On some Intel may be faster, on some AMD.

> I'd hesitate to say windows may be faster, as if it is, it's usually possible

> to modify linux to be as fast.

A large selection of video compression software was quietly bought into by Intel and written optimized for Pentiums. If you are creating mpegs you definitely want a Pentium unless you really know your software. If you are doing anything else, an Athlon on a good motherboard will run much faster for the same price. The top Athlon 55FX costs about \$200 less than the top Pentium. Live with it.

sci.physics: Re: Code breakers beat security scheme of car locks, gas pumps

The fastest Pentium mobo has a 1.2 GHz memory controller. My AMD 55FX has a 2.6 GHz memory controller – inside the CPU not plumbed into the mobo. The much larger and more efficient AMD memory caches mean a lot of the bytes wandering through a Pentium system never leave an AMD CPU until they are done. AMD uses DDR RAM that is wickedly fast at a fair price. Pentiums use DDR2 RAM "that has the potential to exceed DDR RAM in speed" and costs like sin.

Hyperthreading little programs in one Intel CPU can be pretty good. Hypertransport across multiple AMD CPUs is awesome. Four Pentiums will parallelize to about 2X throughput if memory is involved. Four Athlons will give you about 3.96X throughput with at least doubled memory bandwidth vs. single chips. Absent a rigged demo (mpeg compression) AMD waxes Intel's ass Athlon/Pentium and Opteron/Xeon. I've seen no evidence other than Itanium2s being a proprietary dead end. AMD has not commercially gone to 90 nm architecture yet and it still runs cooler than Intel. Intel is doomed.

I've never seen an app ported to both OSs that ran faster in Windows in the same hardware.

NASA built its "Columbia" supercluster with Intel Itaniums. After various public boastings NASA (with crappy performance and a power bill the size of a, well, NASA project) is dumping the Itaniums at warp speed and replacing them, at full added cost, with Itanium2s. Had they used Opteron–800 series or G6s they would have enjoyed massive performance enhancements, a much smaller power bill (including cooling), and a smaller footprint. BTW, smaller means faster all by itself.

--

Uncle Al

<http://www.mazepath.com/uncleal/>

(Toxic URL! Unsafe for children and most mammals)

<http://www.mazepath.com/uncleal/gz.pdf>