Subject: OT:Nforce 650i chipset for native system(DAW)
Posted by Nappy on Mon, 20 Aug 2007 04:30:30 GMT
View Forum Message <> Reply to Message

/>

AASame here, tom tracks only, and then not always. I only have live drums on
final versions, and sometimes I like the racket and leave it in. It's like
.. . . all organic and stuff. :)

S

"Neil" <IOUOIU@OIU.com> wrote in message news:

Subject: Re: OT:Nforce 650i chipset for native system(DAW)
Posted by LaMont on Mon, 20 Aug 2007 04:42:02 GMT
View Forum Message <> Reply to Message

gt; You mean apart from the girl from Finland in the short white dress?
>
>> Kim wrote:
>>> "DC" <dc@spammersinhell.com> wrote:
>>>> While you were gone the Paris NG computer rebooted itself and when it
>>>> came back up, it spit out the secret to life and the universe...
>>> I think I know which moment that was. I was under the shade of a tree
> doing
>>> a painting and smoking a peace pipe when suddenly the truth of everything

Subject: Re: OT:Nforce 650i chipset for native system(DAW)
Posted by Nappy on Mon, 20 Aug 2007 05:20:19 GMT
View Forum Message <> Reply to Message

device: The first and most shocking is that each and every process

What that means: A security vulnerability in any iPhone application can lead
to complete system takeover.
"A rootkit takes on a whole new meaning when the attacker has access to the
camera, microphone, contact list and phone hardware. Couple this with 'always-on'
Internet access over EDGE and you have a perfect spying device," Moore said.

Others agree. "The shellcode combined with the number of bugs present in
the iPhone finally make mobile attacks a real threat," wrote Errata Chief
Technology Officer David Maynor in a blog posting.

and one of a trio who were first to unveil security issues with the iPhone

interview that he wishes he'd been able to use Metasploit when he was writin

---

Subject: Re: OT:Nforce 650i chipset for native system(DAW)
Posted by LaMontt on Mon, 20 Aug 2007 06:28:25 GMT
View Forum Message <> Reply to Message

g
exploits for the gadget back in July.
"It will certainly make life easier" for others who write exploit code for
the iPhone, he said. "Metasploit is the go-to point-and-click [pen-testing]
interface. It's really designed to help you write exploits and deploy [them]
in ways anyone can use. Jailbreak [another development tool] was available
[at the time Miller was writing exploits]. But now [Moore] has Metasploit
where you can right away build payloads that run as executables on the iPhone."

As it is, within three days of the smartphone's July launch hackers cracked
the iPhone's firmware, finding not only that the phone runs on a Unix-like
operating system but going so far as to extract the master root and other
system passwords.
Click here to read more about security issues with the iPhone.
Moore waited until the iPhone price dropped and until the toolchain tool
for iPhone application development was released before he bought an iPhone
to pick apart.
He first installed AppTapp, an iPhone package manager that downloads applications

a VT-100 Terminal to the phone, and voila (after a "few headaches," he said),
he had shell access.
Moore says he can now generate working iPhone shellcode with a version of
Metasploit 3.
Once he had shell access, he found no

Subject: Re: OT:Nforce 650i chipset for native system(DAW)
Posted by Nappy on Mon, 20 Aug 2007 06:33:36 GMT
View Forum Message <> Reply to Message

otential security pitfall in that
its MobileMail application supports Microsoft Office document formats by
using the OfficeImporter framework when converting files into viewable form.
"This looks like a great target for file-format fuzzing and some late-night
reverse engineering," Moore said.

Another potential way for attackers to get into the phone is through the

mDNSResponder service, which runs by default, Moore said. The mDNSResponder, used by iTunes for music sharing, is part of the Bonjour application suite, which provides automatic and transparent configuration of network devices.

When the iPhone first syncs with iTunes, its host name is changed, Moore said. The default hostname becomes "User's iPhone," with the Mac OS X user account name filling in for "User." If the iPhone is connected to a Wi-Fi network, the mDNS service exposes the iPhone owner's user name.
That particular security exposure hasn't yet responded to Moore's probes, he said, making active discovery "less likely."
Moore has also been playing with the "vibrate" shellcode released by Miller at Black Hat 2007. By the time the security show rolled around, Independent Security Evaluators had already revealed, shortly after the smart phone's release, that Apple's popular multifunctional device could be exploited for data theft or snooping purposes.
At the time, Miller, Jake Honoroff and Joshua Mason created an exploit for the iPhone's Safari Web browser wherein they used an unmodified device to surf to a maliciously crafted drive-by download site. The site downloaded exploit code that forced the iPhone to make an outbound connection to a server controlled by the security firm.
The researchers showed that a compromised device then could be forced to send out pers

---

Subject: Re: OT:Nforce 650i chipset for native system(DAW)
Posted by Bill L on Mon, 20 Aug 2007 23:02:04 GMT
View Forum Message <> Reply to Message

s for inserts in the architecture,
so wires is a big hack. Basically what I do is steal 16 words of shared memory at the top of an ESP2 and reserve it. Then for each output wire, I send the audio a sample at a time up to one of the reserved words of memory. For each input wire I retrieve the audio a sample at a time from that reserved word. It's dirt simple, but suffers from a bad side effect. There is no shared memory BETWEEN effects chips. So say that you set up an output wire, and an effect and an input wire, and everything works great. But then you add another effect, and the effects engine shuffles the algos around to different ESP2 chips to get a better allocation. Your input wire can get allocated to one chip, the output to another. Then things no worky. The fix is to remove the input and output wire, then add them back, and in all likelyhood they will end up on the same chip, but its a pain.

I have a great keyed gate and a sidechain I never released because wires is not a reliable method, and there is no other way to route from channel to channel among inserts.

I also can't release the precision limiter because that is the property of one of the original ensoniq guys, and I have an ironclad agreement with him

that I cannot release it, unless its for sale , and he gets a cut.

The one thing I do think we should release is matts reverb, cause nobody has heard from here in years.

Chuck

"Mike Audet" <mike@...> wrote:
>
>No reference projects??!?!?!?!
>
>Chuck, thank you so much for all the work you did. I'm very, very aware
>that I'm blessed to have your work to look at and learn from. I'm having
>such a great time working on this stuff, and it really is a dream come true
>to be able to move PARIS forward.
>
>I've sent you a couple of emails, but I have a feeling that my messages get
>killed by

Subject: Re: OT:Nforce 650i chipset for native system(DAW)
Posted by DJ on Tue, 21 Aug 2007 04:30:19 GMT
View Forum Message <> Reply to Message

y

>>> powerful
>>> editing stuff.
>>>
>>> This new Elastic Audio feature will replace their Beat-Detective feature
>>> which was already a powerful tool for Drum editing..
>
>Hi DJ,
If you are thinking about a single socket 775 board then this one is excellent. It uses the P35 chipset so is compatibel with the 1333mhz fsb chips. It has 3 PCI and 3 PCI-e available. 6 SATA ports, 12 USB, 1 FW, 1 NIC. Very solid board. I've tested thses combinations and it wirked fine. WE only use NVidia vidoe cards so haven't tried ATI or Matrox. Not sure why someone would want to use either of them anyways. :)

3xUAD PCI 1x UAD PCI-e 1x FF800
2x MADI PCI, 2x UAD pci-
