

*Building the Perfect Evil
Twin*

*Rich McGull
Securosis, LLC*

Aren't Evil Twins Old News?

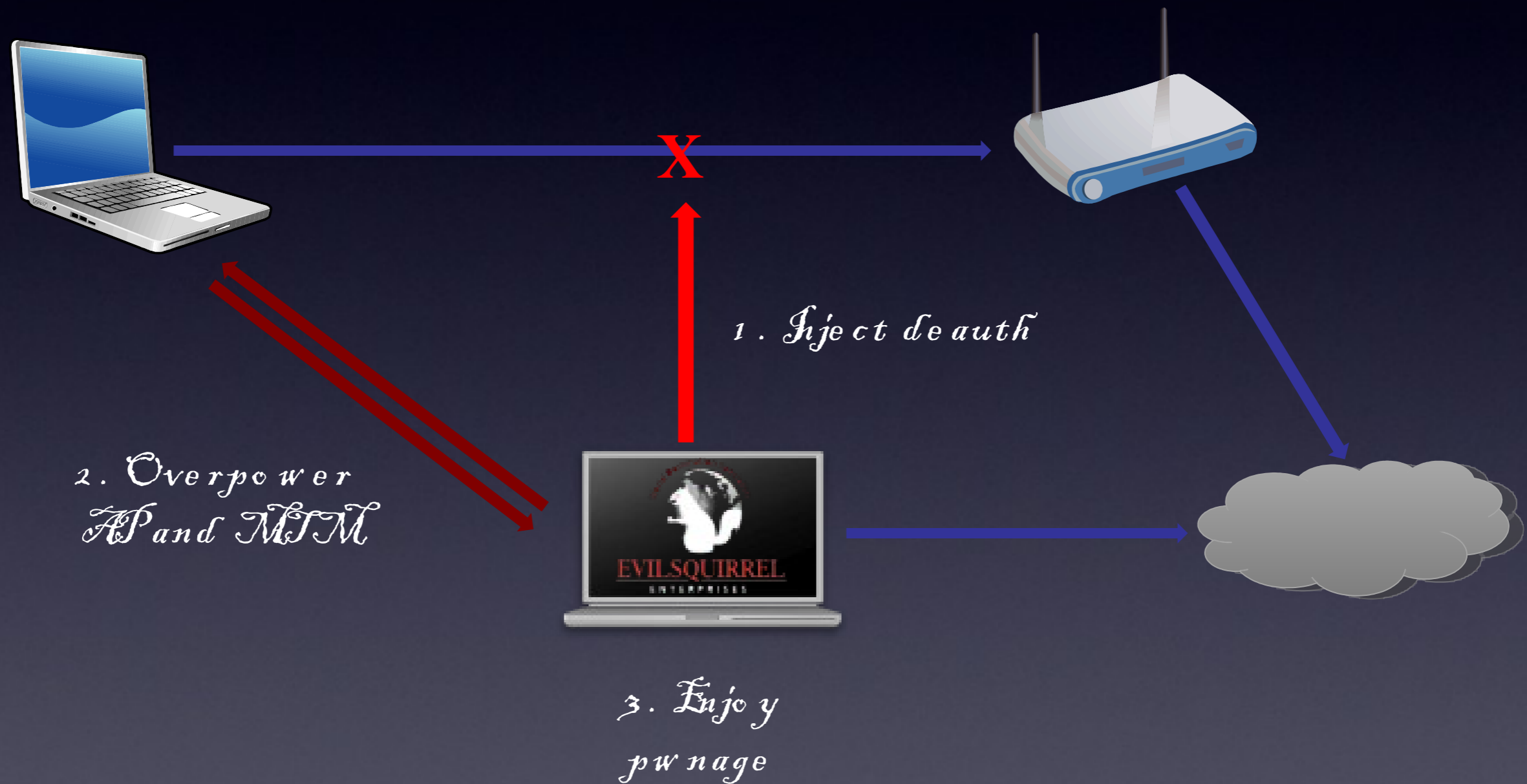
Yep, but so is Jimmy Buffett and he still sells out more shows than god.

Ubiquitous, free,
open, public WiFi

Always-on WiFi
shoved into
every device

Consumerization
of IT

Evil Twin in 101



Evil Twin in 501



- Self contained
- High powered
- Drop and leave
- Multiple exploit options

Exploit Options

- ◊ Exploit browser on splash screen and install trojan for later access.
- ◊ Sniff/MSM traffic.
- ◊ Inject HTML

Why This Matters?

- ◊ *There's nothing new here, but this attack will be effective for years to come.*
- ◊ *It's a great vector for any 0days or other exploit advancements.*
- ◊ *Enterprises are well protected, but distributed enterprises are more vulnerable.*
- ◊ *Pwn the consumer, eventually you own the enterprise.*

Rich Mogull
Securosis, LLC.

rmogull@securosis.com

http://securosis.com

AMsecurosis

Type: rmogull