Rogue Squadron: Evil Twins, 802.11intel, Radical RADIUS, and Wireless Weaponry for Windows

Beetle, beetle@shmoo.com Bruce Potter, gdead@shmoo.com

The Shmoo Group www.shmoo.com



Oh boy, an Overview!

- Wi-Fi threats from old to... old?
- Rogue APs: basics to badass
 - EAP Peeking, Two-factor Terrorism
- Wireless Weaponry for Windows
 - Airsnarf for Windows, Rogue Squadron
- Rogue AP defense
 - HotspotDK, sage advice from the Shmoo
- Q & A

Why oh why do we Wi-Fi?

- Who here has an open wireless network at home?
- Who here has an open wireless network at work?
- Crap! My Tivo can't do WPA. Neither can my PSP. Ummm... does it matter?
- When and where should we Wi-Fi?
 - Coffee Shops? Airports? Hospitals?Banks? Ummm... Nuclear Power Plants?



standards. The same infrastructure also will provide wired LAN connectivity throughout the plant for both voice and data applications as well as for remote video monitoring and control

According to Carter, TXU plans to use the wireless solution—provided by Azima—to help Comanche Peak integrate its work order management and scheduling processes, electronic procedures, clearance and safety tagging, operator logs, equipment monitoring, electronic messaging, plant drawings, phone books, equipment references and locations, and selected Internet/intranet access. Video applications will include radiation protection monitoring, remote equipment monitoring, and video conferencing.

So far, Azima has installed monitoring



4. Collecting the data. A typical wireless access point at Comanche Peak. So far, Azima has installed monitoring devices on more than 50 pieces of critical equipment within Unit 2. Courtesy: TXU

devices on more than 50 pieces of critical equipment within Unit 2 of Comanche Peak. Besides vibration, the devices also monitor current, partial discharge, motor speed, and other key variables. Other wireless applications already installed throughout the plant include mobile computing, video monitoring, and VoIP telephones (Figure 4).

More wireless implementation stories

Two other projects underscore the growing popularity of wireless machinery monitoring. One is at Exelon Nuclear's Limerick Generating Station (Figure 5) in Montgomery County, Pa. The Limerick plant has had maintenance problems with the fans used to exhaust turbine enclosures. Nicknamed "fans-in-a-can" because they are typically mounted inside cylindrical ducts, these fans are inaccessible to technicians while the plant is on-line. But since the installation of transmitter-equipped vibration and temperature sensors on the fans' motors. Limerick has seen reductions in the time and costs of document control and tracking, data conversion/transcription, and error checking/reduction.

The other wireless monitoring project worth mentioning was at the San Onofre Nuclear Generating Station in California. Engineers at the plant had long wanted to remotely monitor the temperature of several 2,500-hp secondary plant motors as an indicator of their health. According to Lloyd

Pentecost, a maintenance engineer at the plant, "If a motor were to fail unexpectedly, the plant would have to operate at only 80% capacity for a number of days, and the losses could exceed \$400,000." Pentecost is pleased with the network of wireless temperature sensor/transmitters that has been installed at San Onofre because "Collecting and analyzing motor temperature data in real time allows action to be taken before a catastrophic failure occurs."

EPRI promotes wireless

The Comanche Peak de-wiring project was executed in partnership with EPRI, which set up the performance benchmarks and monitored the project. EPRI plans to issue a comprehensive report on it this summer.

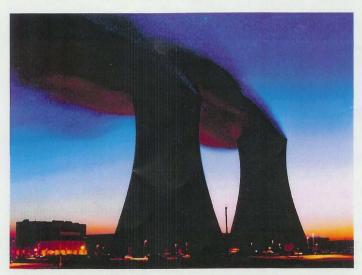
Ramesh Shankar, who is spearheading an EPRI program to evaluate the feasibility of installing more remote monitoring systems at U.S. utility generating stations, believes that wireless is a technology whose time has come. He says a major focus of the effort is to determine the extent to which wholesale deployment of wireless devices might improve plant safety and reliability.

Shankar adds that his program already has two "products." One lays out the business case for applying wireless technologies; the other offers advice to plant managers on implementation and regulatory issues. To support the effort, EPRI has formed a Wireless Technology Working Group to develop guidelines and to help member companies achieve reliable, economical, and safe use of wireless devices. EPRI also has helped the DOE's Oak Ridge National Laboratory form the Wireless Industrial Networking Alliance (WINA). The mission of WINA is to promote a dialogue among suppliers, end users, and government about wireless technologies in the nation's power plants.

To accelerate the adoption of wireless technologies for machinery monitoring and data/voice/video communications, WINA is focusing on four different activities:

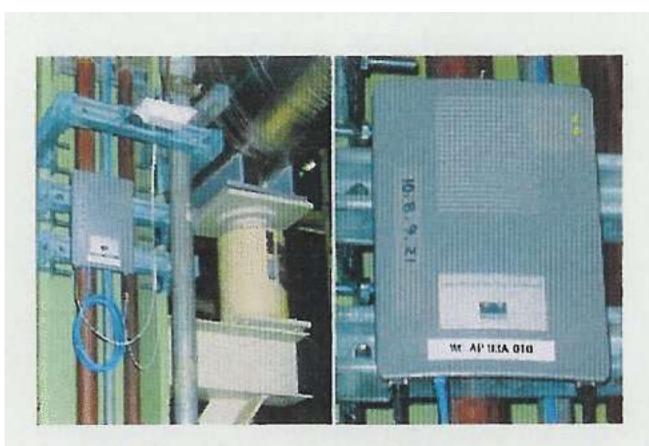
- Explaining wireless technologies to end users.
- Promoting effective standards, regulations, and practices.
- Quantifying and communicating the benefits of going wireless.
- Benchmarking against customer requirements.

Each year, WINA sponsors two wireless workshops that are focused solely on the power generation industry. The next one is scheduled for October 3–5 in Jersey City, N.J. m



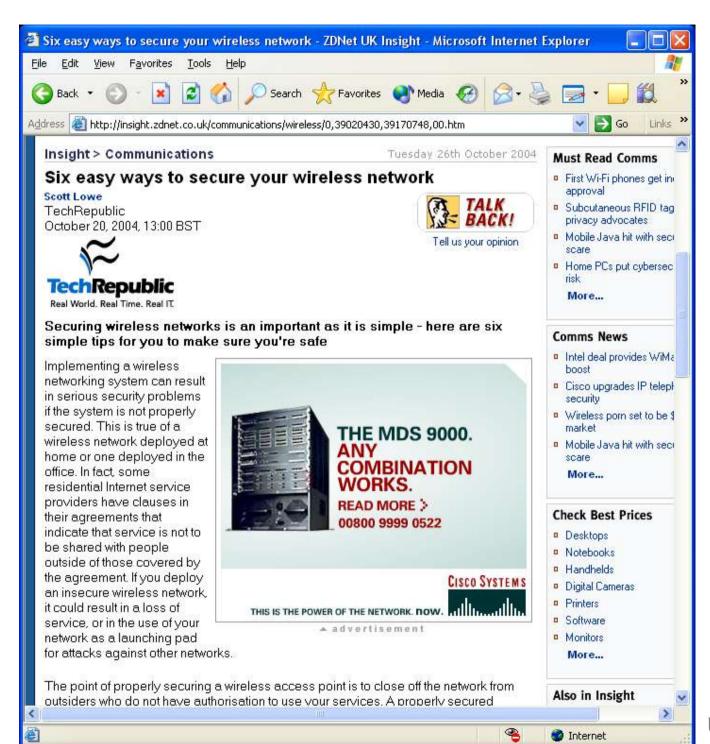
5. Watching those "fans in a can." At Exelon Nuclear's Limerick Generating Station, wireless technology is being used to monitor inaccessible fans and motors. *Courtesy: Exelon Nuclear*





4. Collecting the data. A typical wireless access point at Comanche Peak. So far, Azima has installed monitoring devices on more than 50 pieces of critical equipment within Unit 2. Courtesy: TXU











Where did we go wrong? Where are we going?

- Technology of convenience versus the inconvenience of securing it.
- The poor, poor users were left out in the authentication cold.
- Half-ass security standards pass the buck and / or provide defacto insecure options.
- Security acronyms have taken precedence over proper implementation.

 BLACK HAT, USA, 2005



"CHOOSE A MOBILE NETWORK AT RANDOM!"



Club World, More beds, more places, more often.

Hello Switch to Radiolinja for Elisa, the Vodafone network in Finland.

How the FUCK does the user know?!



Rogue AP 101

- Traditional thought = corporate network backdoor
 - Unauthorized AP plugged into Intranet
- A la Airsnarf, usernames & passwords for websites (or worse) can be stolen
 - Attacker runs enticing / duplicate AP
 - User associates to AP that has duplicate SSID, websites "appear" to be legitimate





Access Point



SSID: "goodguy"

Stronger or Closer Access Point



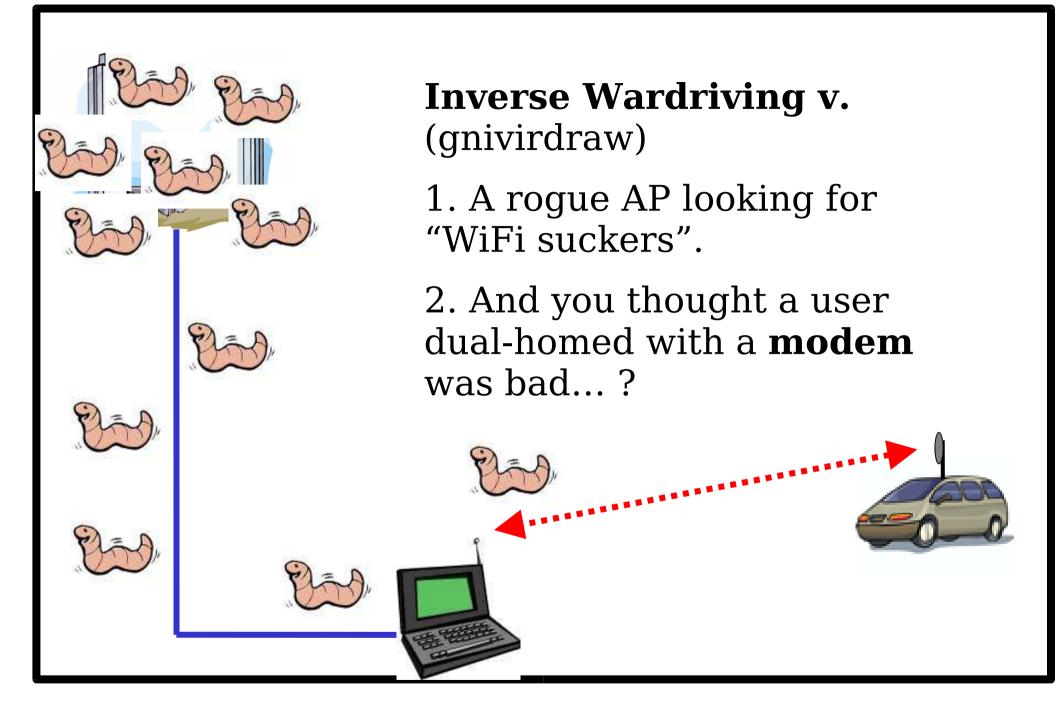
SSID: "badguy"



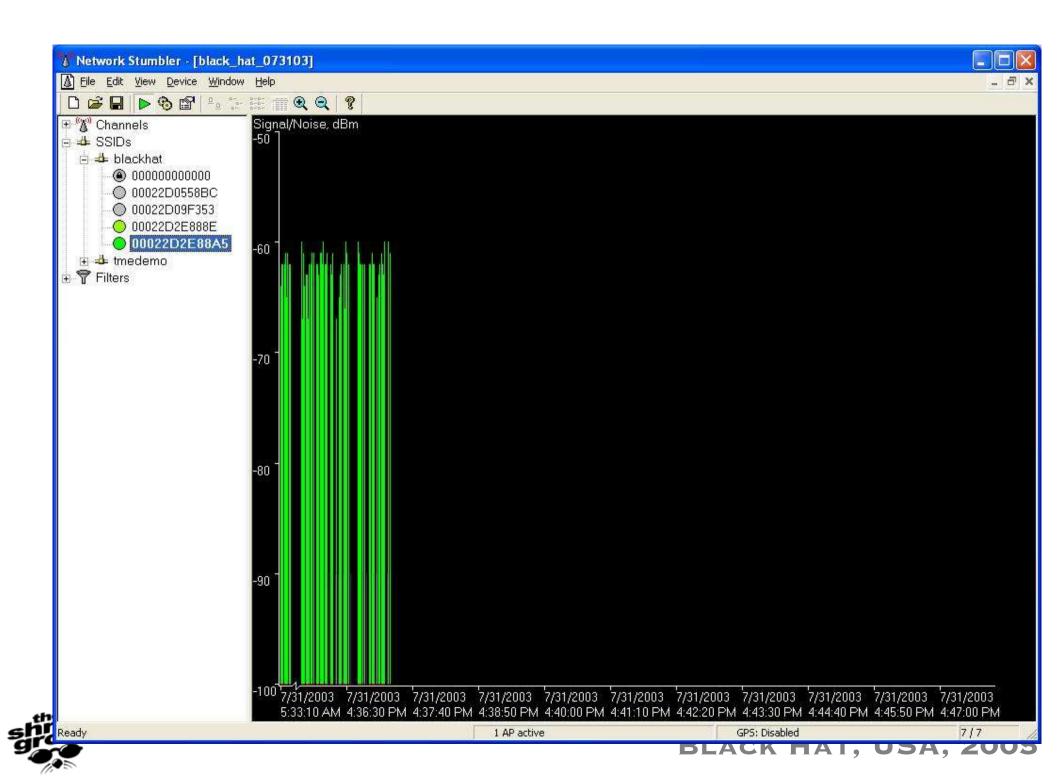
Wi-Fi Card

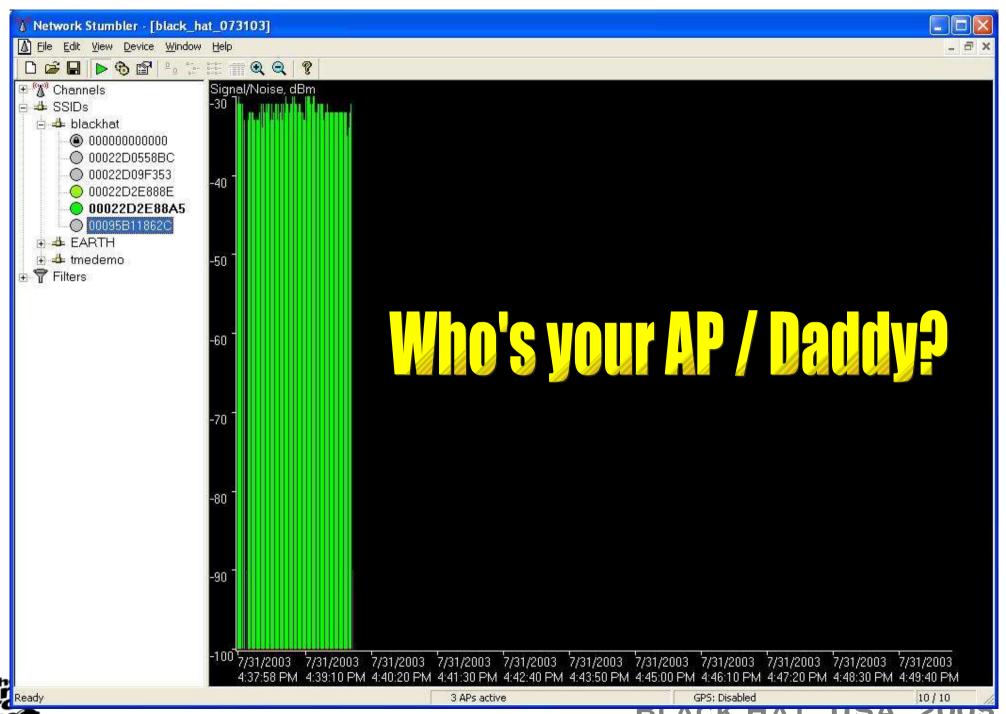
SSID: "badguy"









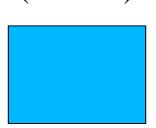


Rogue AP Attacks

Choose your Wi-Fi weapon...

Cisco Gear @ 100mW (20dBm)

Normal Gear @ 25mW (14dBm)



Senao Gear @ 200mW (23dBm)

Use a 15dBd antenna with a Senao for 38dBd total...

6 WATTS!

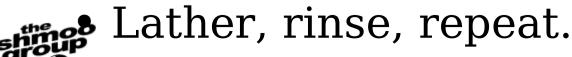
VS 25mW?

BAD GUY WINS! NO CONTEST!



Rogue AP How-To

- Use a hostap compatible wireless card to create a competing access point
- Provide IP, gateway, DNS
- Resolve all websites to your address, or NAT and selectively provide fake DNS replies
- Dynamically display fake websites for popular URLs via virtual hosting





Badass Backends and Two-Factor Terrorism

- Web-based authentication via wireless is an unholy marriage of two technologies—provides new attack vectors.
- Two-factor authentication can not even save you. Yes, this means 0wning SecureID via rogue AP is possible.
- Username, PIN, and token can be snarfed and used in REAL TIME!



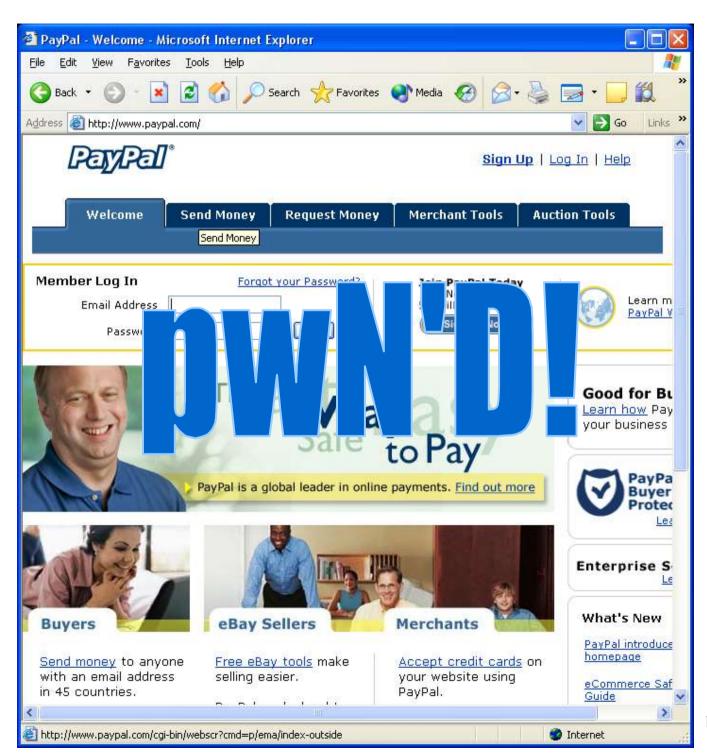
Badass Rogue AP Attack Demo





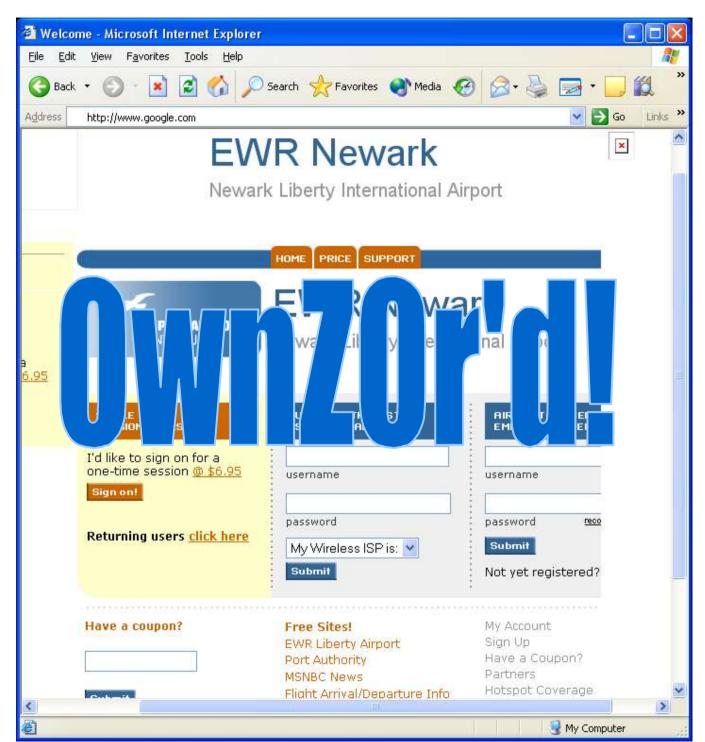


USA, 2005





USA, 2005





USA, 2005

Rogue APs won't go away...

- Users will be users, and they WILL fall for access point "impersonators".
- If you didn't notice, phishing and identity theft are on the rise... and so is hotspot usage.
- "Extra" wireless client profiles provide extra avenues of attack.
- EAP is an acronym, not a catch-all.
- Gartner can blow us.



802.11intelligence

- What other bits of info are users giving away via wireless?
 - Domains
 - Shares
 - Proxies
 - Installed software
 - Other preferred wireless networks
 - More?



What about EAP-secured wireless networks?



All Your EAP

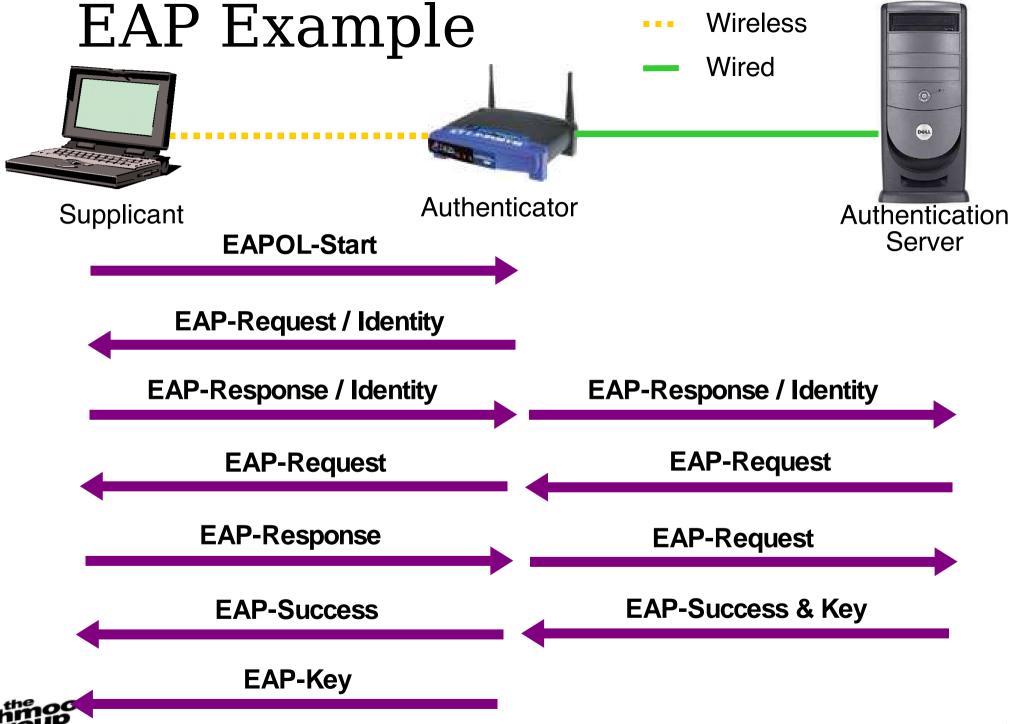
- Oh crap. The EAP acronym bonanza:
 - EAP-MD5-Challenge, EAP-MSCHAPv2, EAP-GTC
 - EAP-SIM
 - FAP-TLS
 - EAP-TTLS (w/ MD5-Challenge, GTC, MSCHAPv2, PAP, CHAP, et al. variants) by Funk
 - LEAP, EAP-FAST by Cisco
 - PEAP (w/ MSCHAPv2, MD5-Challenge, GTC variants) by Microsoft et al.
- Lots of ways to screw this up. But first...



EAP for Dummies

- Three major components:
 - Supplicant = User / Client
 - Authentication Server = Duh. RADIUS fits here.
 - Authenticator = Device in between the two.
- Authentication goes something like this:
 - EAP-Request / Identity to Supplicant from Authenticator
 - EAP-Response / Identity to Authenticator from Supplicant which gets passed to Authentication Server
 - Challenge / Response brokered, and if successful authentication, then Authenticator allows Supplicant access to network based on what Authentication Server say is appropriate.





BLACK HAT, USA, 2005

Rogue APs vs EAP Security?

- EAP security really only comes in to play with its tunneled variants that use TLS.
- Two basic goals in mind with the "secure", credential-tunneled variants of EAP:
 - Give the supplicant a way to authenticate the authentication server so they don't go spilling their guts to the wrong guy.
 - Create a secure tunnel so that the supplicant and authenticator can have a secure challenge / response exchange mechanism, which can also be used to pass dynamic keying material.

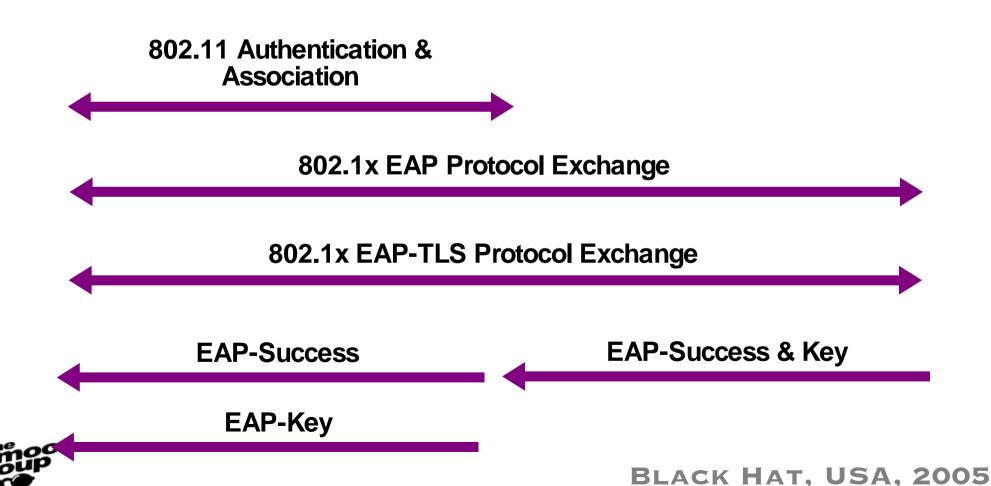


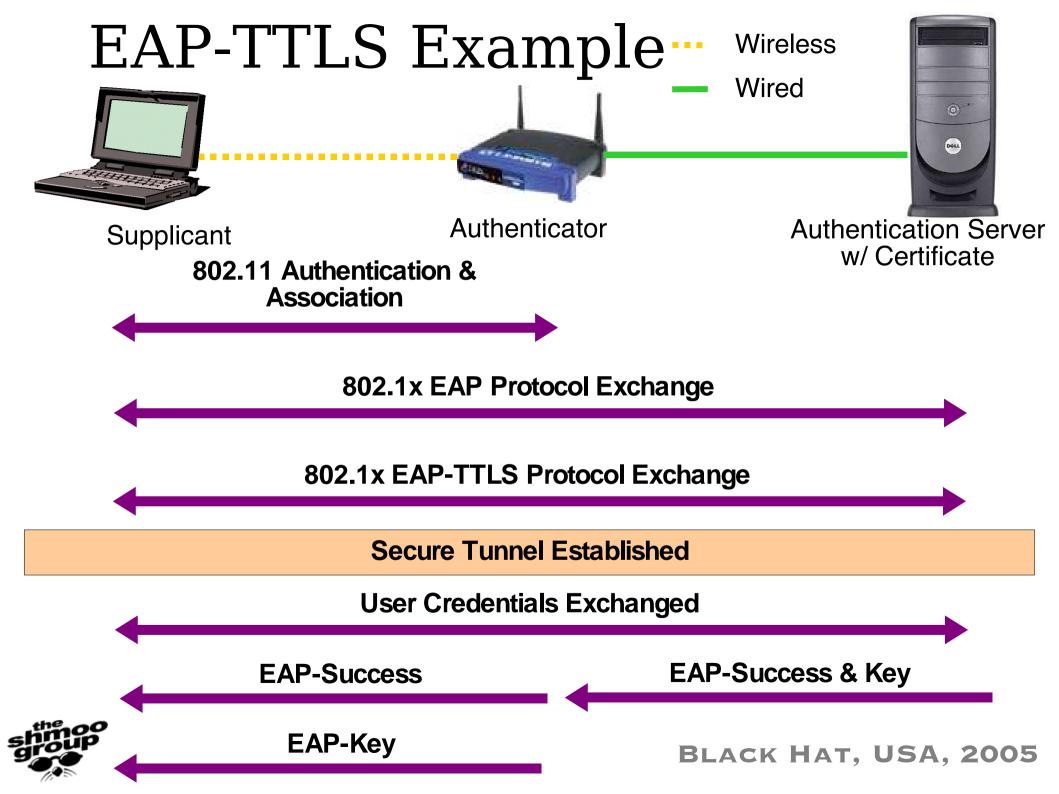
Rogue RADIUS

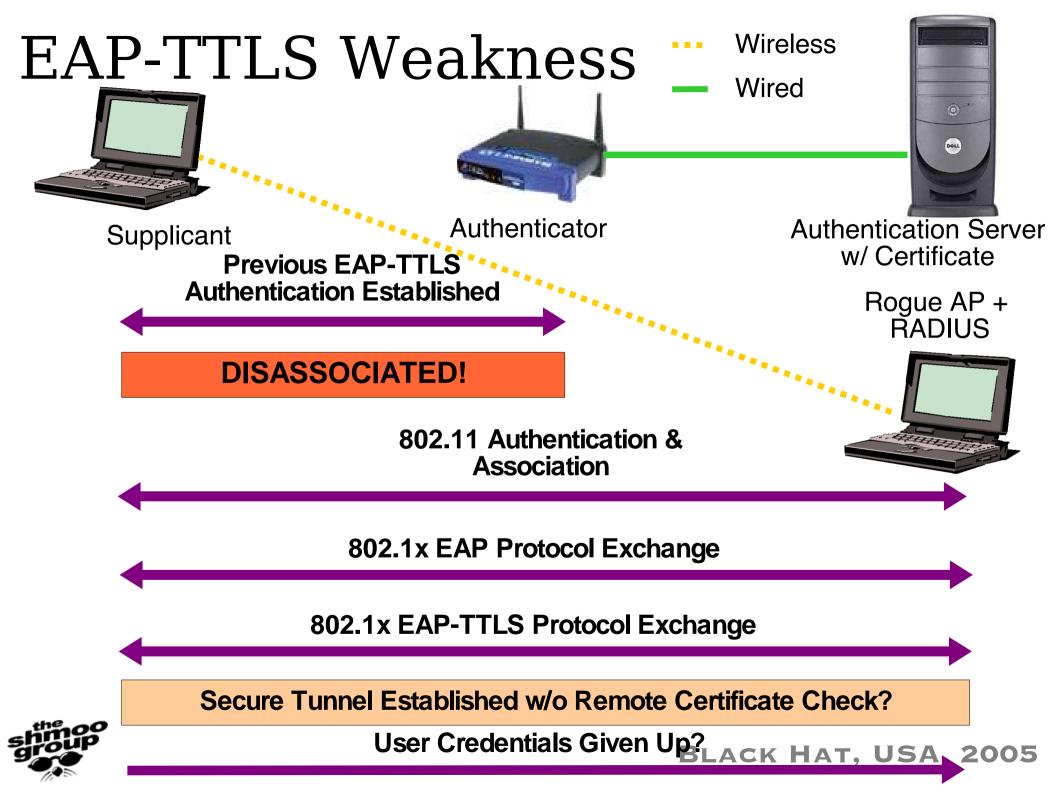
- Who says rogue APs can't be used against corporate wireless networks that employ EAP?
- As we said, there are plenty of ways to screw up EAP. Thanks vendors!
- FreeRADIUS provides a simple & easy way to accept EAP credentials
 - Integrates nicely with hostapd.
- Can allow for "EAP Peeking"...



EAP-TLS Example Wireless Wired Supplicant w/ Certificate Authenticator Authentication Server w/ Certificate







All Your PAP... Google for targets, if you like.;)





Wireless

Wired

EAP-TTLS w/ PAP Attack?



Windows XP SP2



EAP-TTLS w/ PAP over TLS





RADIUS Server

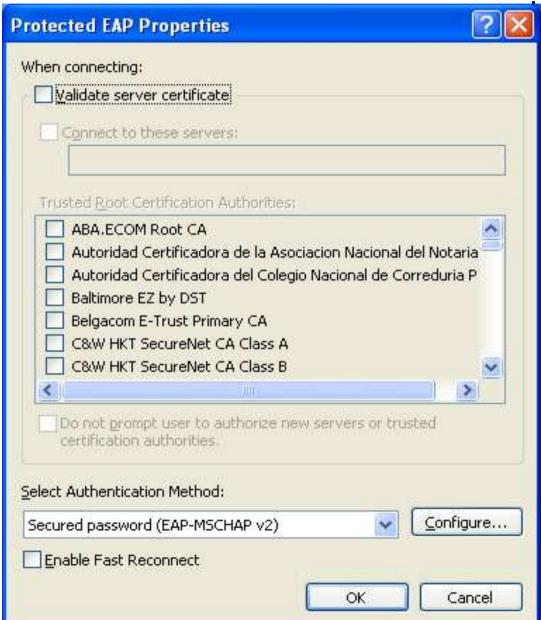
- 1. Disassociate users.
- 2. Learn username & password.
- 3. Disassociate, copy creds to local EAP config.
- 4. Impersonate victim with legit username & password whenever.



Rogue AP w/ Rogue RADIUS Server



All Your CAs... The "All or None" Vulnerability





НАТ, USA, 2005

••• Wireless



PEAP Attack?



Windows XP SP2



PEAP w/ MSCHAPv2 over TLS



Rogue AP w/ Rogue RADIUS Server



RADIUS Server

- 1. Disassociate users.
- 2. Learn DOMAIN and username w/ rogue AP.
- 3. Disassociate, seed local password file.
- 4. User continuously attempts to reauthenticate.
- 5. Repeat #3.
 Authentication success
 = correct password
 guessed!



Wireless Weaponry for Windows

- But rogue AP attacks require a "sophisticated hacker", right? Wrong.
- SoftAP + TreeWalk + Apache + ActivePerl = Airsnarf for Windows
 - http://airsnarf.shmoo.com/airsnarf4win.html
 - "Evil Twin Access Points for Dummies"
- But why only run one rogue AP, when you can run two... or three?



Rogue Squadron Demo



Is there no defense?



Status Asso	ociated - 00:02:20):05:58:BC
Current Channel	<u>[11</u>	Rescan
Current Tx Rate	11 Mbits/se	c Disable Radio
Throughput (Byl	tes/sec)	
Tx 56	Rx	1176
Signal Strength:	Good (66%)	
HINERALD		
Link Quality:	Excellent (80	%)
-		







Defending Wireless Networks

- We seemed to have covered a lot of ground on the Offensive.. What about Defense *boom boom* Defense!
- Multiple issues afoot... need a solid grasp of network engineering, security, and user needs/will
 - Architecture and Configuration
 - Protecting the enterprise and Protecting the Client
 - Secure and Security Operations



Wireless Architecture

- Many options... maybe too many
- First, need to understand how network and system architecture impacts wireless security
- Layered defenses are a good way to start...
 - Some folks just secure layer 2
 - Some folks just secure layer 3
 - Some folks do both
- What's the right solution?



Protecting Just Layer 3 is a Bad Idea

- The goal is not to JUST protect the traffic
 - But that's all Layer 3 protection really buys you
- Does NOT protect a client from layer 2 tricks such as Rogues
 - The impact of Rogues may be mitigated, but depending on how good/bad the VPN software is, they may still be tricked
- Does NOT protect the infrastructure
 - Bad network architecture (leaking STP, CDP, routing info, shared LAN segment, etc) can still lead to compromise.



Protecting Just Layer 2 is a bit Better

- Using Layer 2 authentication and encryption (if done right) prevents most attacks on the client AND infrastructure
 - For instance, if you're leaking STP, at least it's encrypted
- But, note the previous 40 slides.. Layer 2 security is hard work



Protecting Both is a lot of work

- But, it's really your best defense
 - So, play the risk/reward game
- Given my option, I'd put my money on Layer 2 and get that RIGHT before spending money on layer 3



Configuration

- Don't screw up your wireless configuration
 - Cost of failure is high
- Don't screw up your client configuration
 - Cost of failure is high
- Even proper configuration does not ensure a secure network or client
 - Bad code in VPN or ESP software, for instance, could sink the whole thing anyway



Securing the Client or the Infrastructure?

- Just in case you missed it, your Enterprise 1x solution does not protect your client machines on the road
- Need Client software that can detect and defend against rogue AP attacks
- TSG released the Hot Spot Defense Kit at DC BH 03



Defending Wireless Networks

- At the time of HSDK, there was NO capability for rogue detection in commercially avail software
- Today, we're still not much better
 - AirDefense Mobile, some other small stuff
 - Rogues are THE BIGGEST threat against enterprise networks
- So, while the industry is still finding their whatnot with both hands, we're making...



Hot Spot Defense Kit v2

- Enterprise wireless IDS systems look for any attack, not just one directed at a particular client
- When you are on the road (or don't have the "luxury" of an enterprise WIDS) you need the same kind of protection
- HSDK v 2 aims to be an environmental monitor of sorts
 - Looks for any zip in the wire, not just ones directly effecting the client
 - If you're in downtown Baltimore, and someone starts shooting, you tend to freak out even if they're not shooting at you... wireless shouldn't be any different

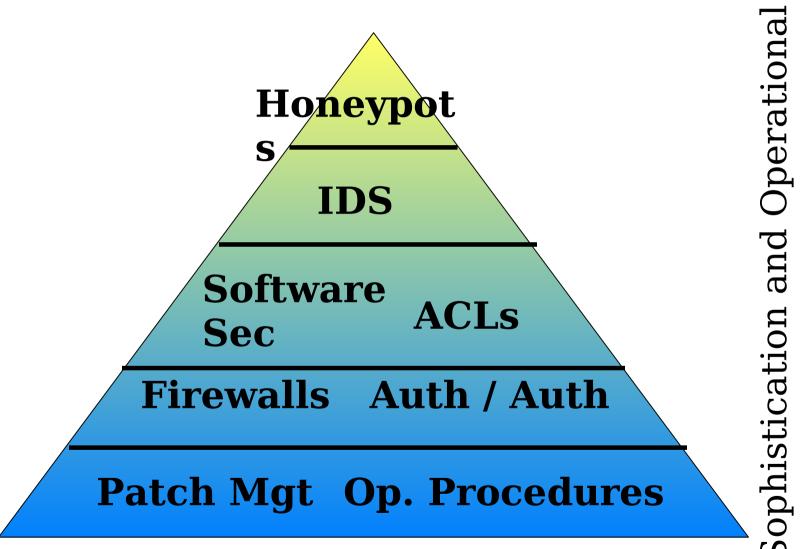


HSDK v2

- Still under development
- Looking for:
 - Mass auth/deauth/assoc attacks
 - Fake AP signatures
 - Reinjection attacks (hard)
 - Bluetooth attacks (wireless isn't just .11, ya know)
 - The standard rogue detection stuff from v1
- If something is detected, the green ball turns red (step away from the computer)
 - If security software isn't usable, it's useless
- http://airsnarf.shmoo.com



Secure vs Security Operations





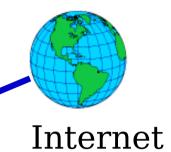
What's in YOUR wireless network?





Wired

Example



AP w/ WPA-PSK using AES



DMZ



Cable / DSL Router

Trusted

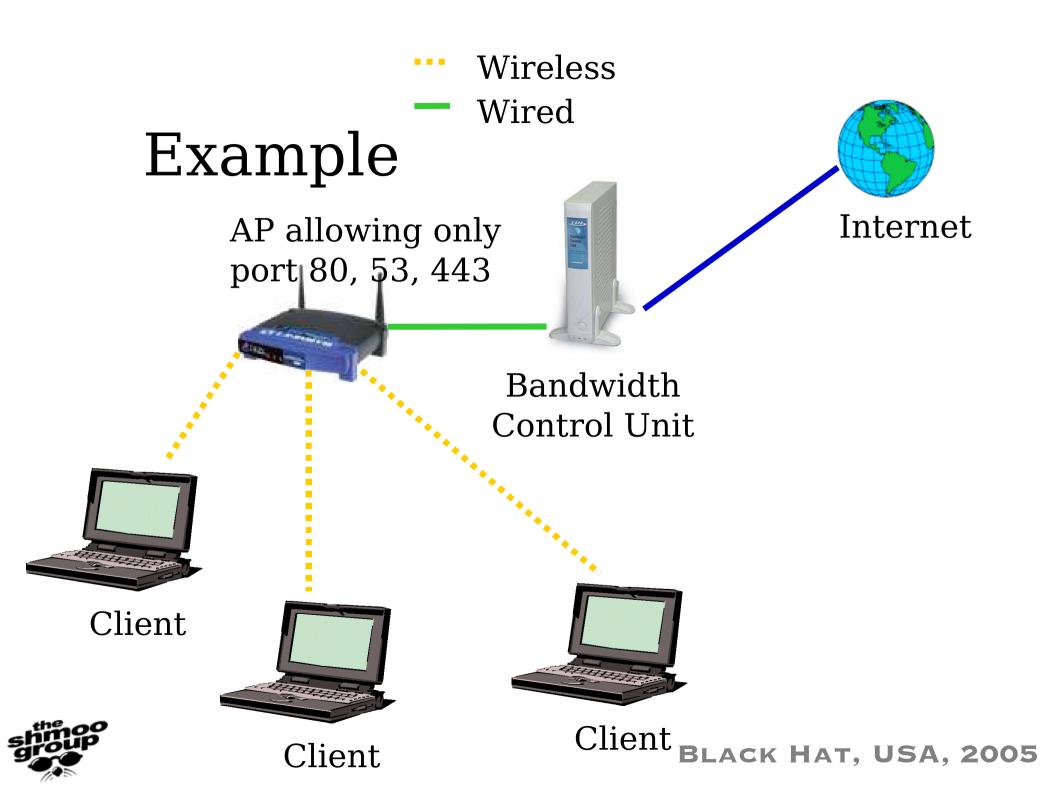


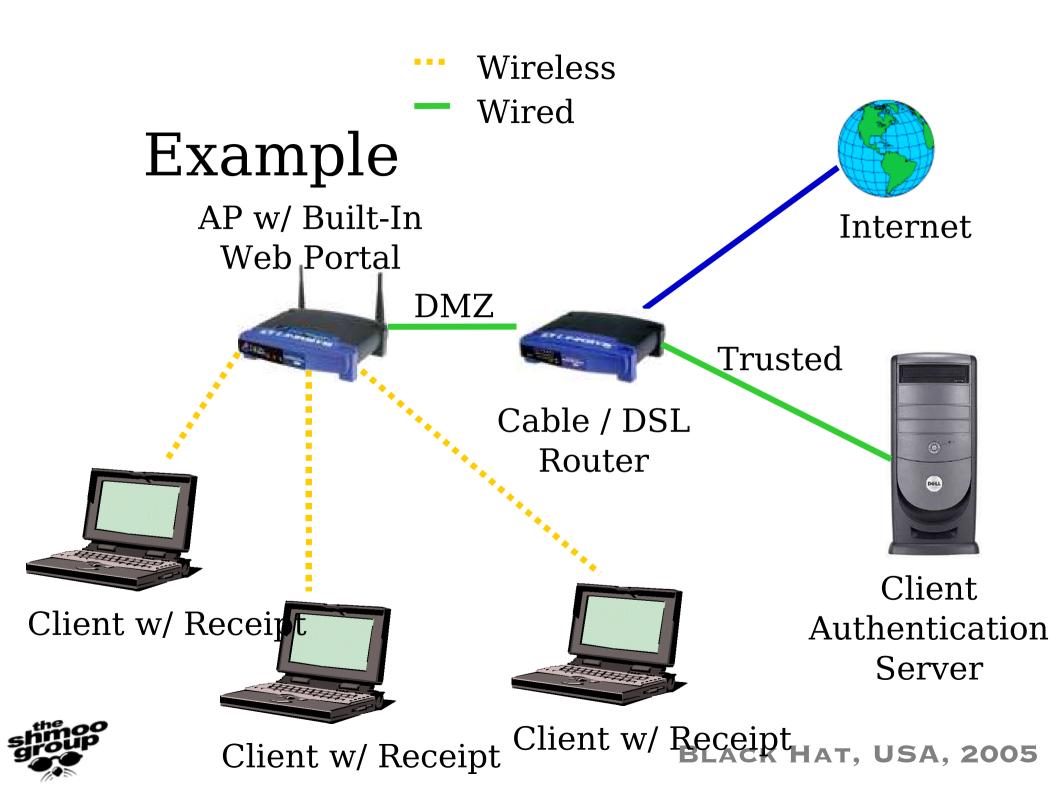


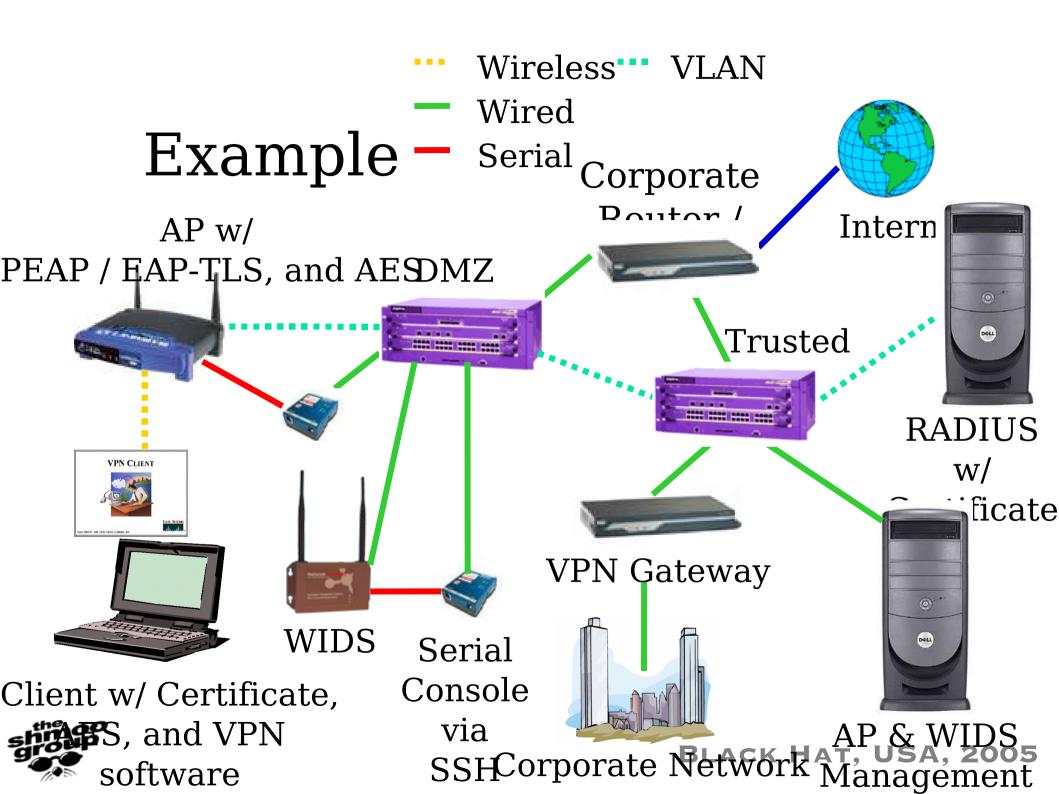


BLA Home-Networkos

t w/ WPA-PSK using AES







More WMI 4 U

- Trying to get a handle on wireless, but all you are is a Windows network administrator? Perfect.
- WMI allows you to do some nifty things.
 - Scan for SSIDs
 - Check for dual-homed wireless users
 - Find rogue APs?



See Beetle's ToorCon 2004 presentation.

BLACK HAT, USA, 2005

17 line SSID Scanner for Windows in VBScript

```
on error resume next
set objSWbemServices = GetObject("winmqmts:\\.\root\wmi")
set colInstances = objSwbemServices.ExecQuery("SELECT * FROM
MSNDis 80211 BSSIList")
for each obj in colInstances
   if left(obj.InstanceName, 4) <> "WAN " and right
(obj.InstanceName, 8) <> "Miniport" then
      for each rawssid in obj. Ndis80211BSSIList
          ssid =
          for i=0 to ubound(rawssid.Ndis80211SSid)
             decval = rawssid.Ndis80211Ssid(i)
             if (decval > 31 AND decval < 127) then
                 ssid = ssid & Chr(decval)
             end if
          next
          wscript.echo ssid
      next
   end if
next
```



Summary

- Implementations vs Acronyms
 - "EAP" and "VPN" sound great—did you get them RIGHT, though?
- Configuration management of user wireless profiles
 - Rule with an iron fist or DIE!
- Why do you Wi-Fi?
 - It's OK to say "NO" if it's not a "good fit".



Wireless threats vs \$\$\$?

Links

- http://airsnarf.shmoo.com/
- http://airsnarf.shmoo.com/rogue_squadron/
- http://hsdk.shmoo.com/
- http://www.shmoo.com/
- And the next con you should be planning on attending is ToorCon!
 - http://www.toorcon.org/



Questions?

