

---

---

---

---

---

---

---

---



---

---

---

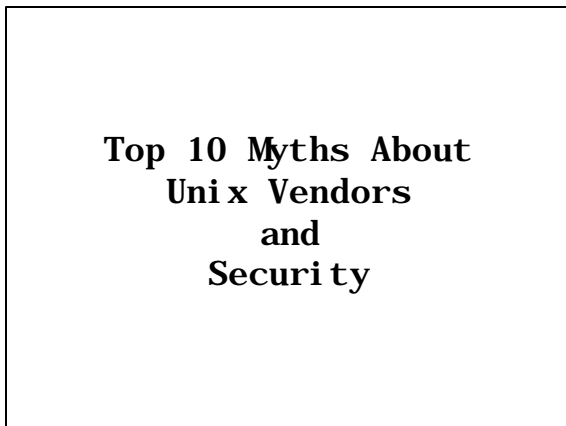
---

---

---

---

---



---

---

---

---

---

---

---

---

**- MYTH 10 -**

**Vendors NEVER respond when sent a security problem**

- >We do read BugTraq and friends
- >>50% of what we receive is B.S.
- >SPAM, SPAM, SPAM . . . and Klez!



---

---

---

---

---

---

---

---

**- MYTH 9 -**

**Those vendors take FOREVER to respond.**

- >A month is NOT 6 days
- >We can't retaliate...even to the "respectable members of the security community"



---

---

---

---

---

---

---

---

**- MYTH 8 -**

**Vendors do NOT fix things.**

- >"I read on BugTraq that you fixed this problem."
- >Do you **really** believe everything you read?



---

---

---

---

---

---

---

---

**- MYTH 7-**

**If you would only write GOOD software.**

- >My girlfriend insists on this question:
- >How many of you have been developers?
- >Export Control
- >Third Party Storage
- >Hardware Bugs, anyone?

---

---

---

---

---

---

---

**Hardware Bugs**



- >Non Exec Space Stacks in CPU Design
- >FIPS-180 Randomness
- >Statement of Volatility
- >TOE, SSL Acceleration
- >Hardware Engineers (E.E.'s)

---

---

---

---

---

---

---

**- MYTH 6-**

**Unix Vendors work with intrusion detection and host hardening vendors.**

- >When ISS says something...
- >Scanner reports no problems but...
- >Scanner Vendors and Unix Vendors do NOT talk to one another.



---

---

---

---

---

---

---

**- MYTH 5 -**

**Vendors are against FULL DISCLOSURE.**

- >Full Disclosure is NOT Immediate Disclosure.
- >Graduated Disclosure is BAD
- >#include <snmp-horror-story.h>
- >Recent RFC not instituted by Microsoft.
- >OIS, the Organization for Internet Safety and beyond.

---

---

---

---


---

---

---

**- MYTH 4 -**

**Silence is GOLDEN.**



- >2 Years Ago: Shells and TMP files.
- >Situations that PRESSURE vendors to keep silent even when they do NOT want to...
- >COMPAQ / SnoSoft fiasco (even before the evil DMCA was thrown into the mix).

---

---

---

---

---


---

---

**- MYTH 3 -**

**When a vendor says "Security" this is "Security" as you or I understand it.**

- >C2/B1
- >Common Criteria Evaluation
- >Oracle Unbreakable
- >And when marketing talks: "This stuff sells!"



---

---

---

---

---

---

---


**- MYTH 2-**

**Customers are actually explicit in asking for a patch.**

>"I just want a patch/fix **DAMMIT!**"

><irony>No one ever wants *exactly* what they are running now with *just* a security fix. </irony>

>Yes, people have good reason not to want to upgrade...



---

---

---

---

---

---

---

---

**What is the  
Number 1  
Myth?**

---

---

---

---

---

---

---

---

**- MYTH 1-**

**Customers tell us security is their NUMBER 1 Priority.**

>The Number 1 Priority is:

✦

**UPTI ME**

And some folks accept rebooting Windows every day.

---

---

---

---

---

---

---

---