Dirty Little Secrets of Information Security

Why we might not be doing as well as you would hope.

Bruce Potter (gdead@shmoo.com)

Don't Believe Anything I Say

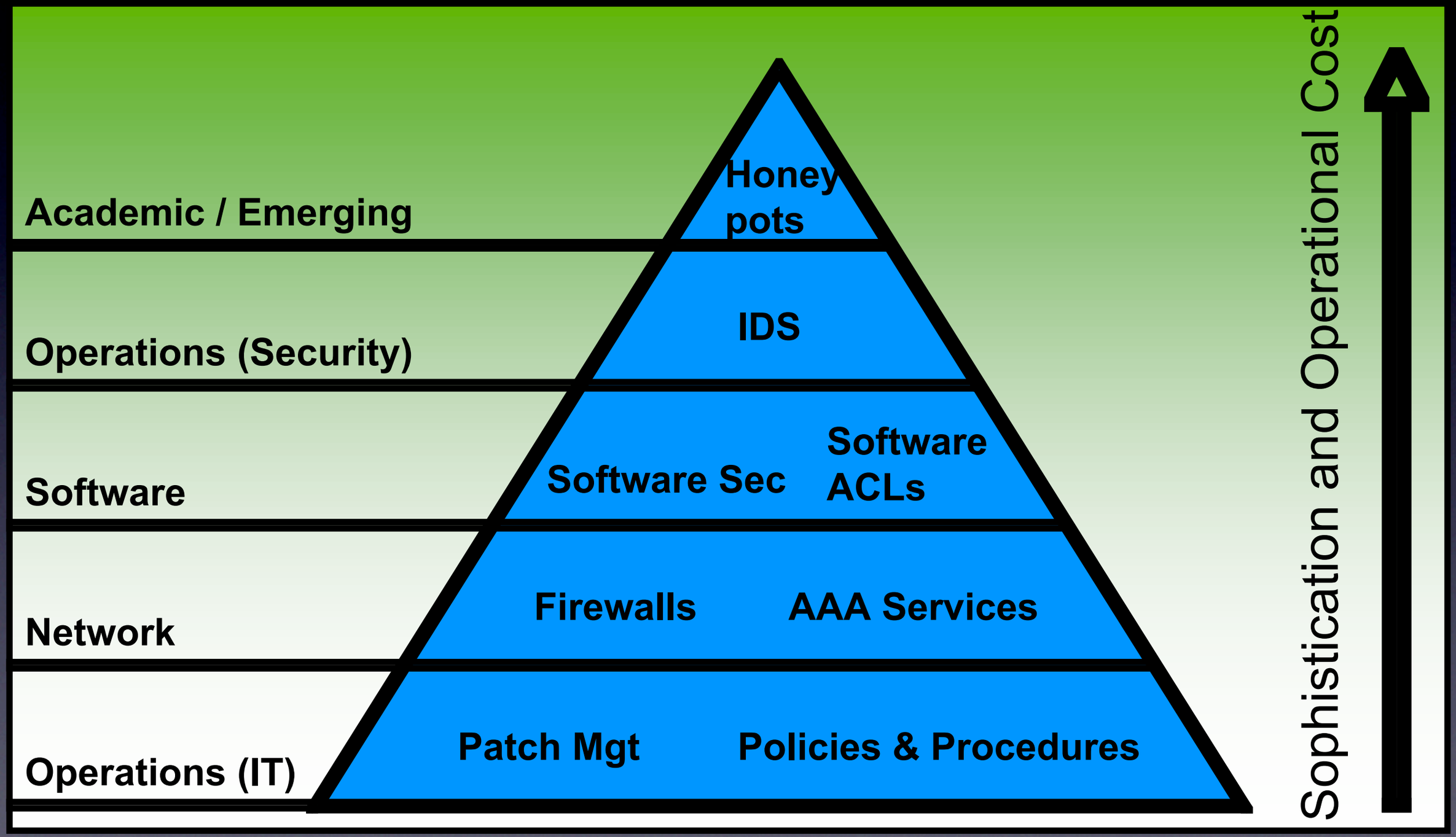
- *"Every person who has mastered a profession is a skeptic concerning it."* - **George Bernard Shaw**
- *"Authority has every reason to fear the skeptic, for authority can rarely survive in the face of doubt"* - **Robert Lindner**

- Security is all about not trusting what you are hearing, seeing, or being sent to you
  - As true in meatspace as in teh tubes
- By Day, Senior Associate for Booz Allen Hamilton
- Wireless Security, application assurance, information security strategy
- By Night, Founder of The Shmoo Group

What's happening here?

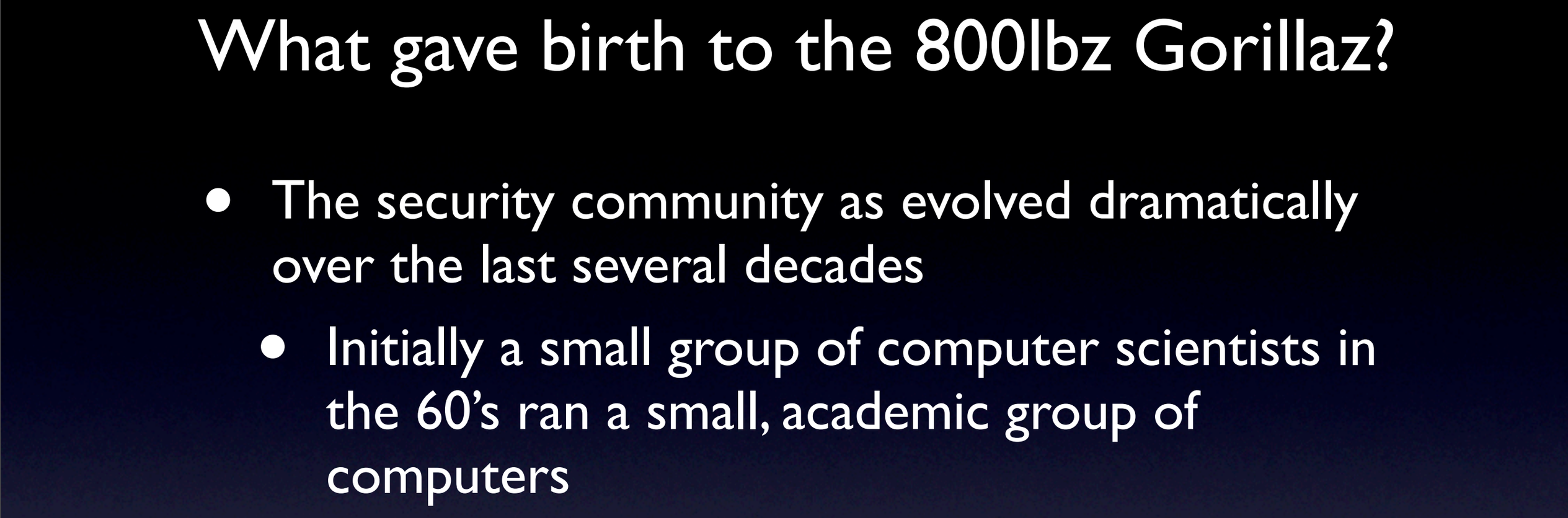
- The goal of this talk is to call out some of the 800lbs gorillas in the room
  - The security industry is riddled with them, and sometimes they're called out in non-productive ways
  - I'd like to address them head on... and actually do something useful with our jobs
- NOTE: Much of what is in this presentation you will probably disagree with. Also, much of what is in this presentation is my opinion and analysis based on what can loosely be called "research." Feel free to throw stones.

Let's have some structure to our discussion



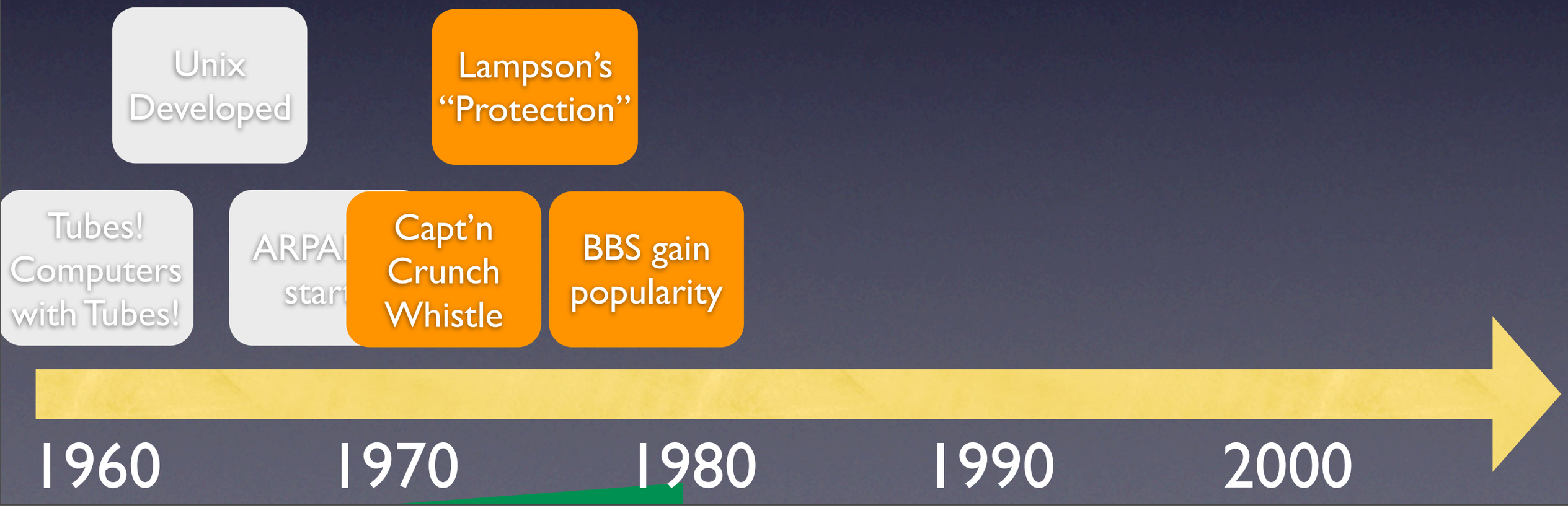
What gave birth to the 800lbz Gorillaz?

- The security community as evolved dramatically over the last several decades
  - Initially a small group of computer scientists in the 60's ran a small, academic group of computers



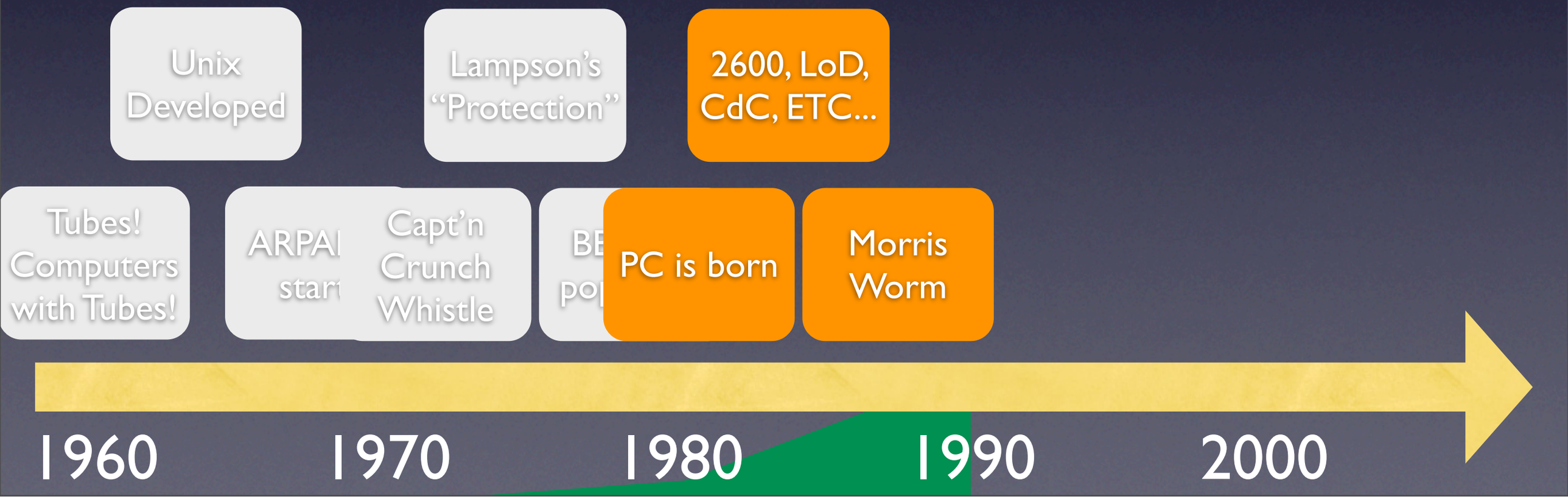
What gave birth to the 800lbz Gorillaz?

- Things got serious in the 70's
  - Telnet was introduced
  - A great deal of research on trusted systems was performed
  - Blueboxing was born



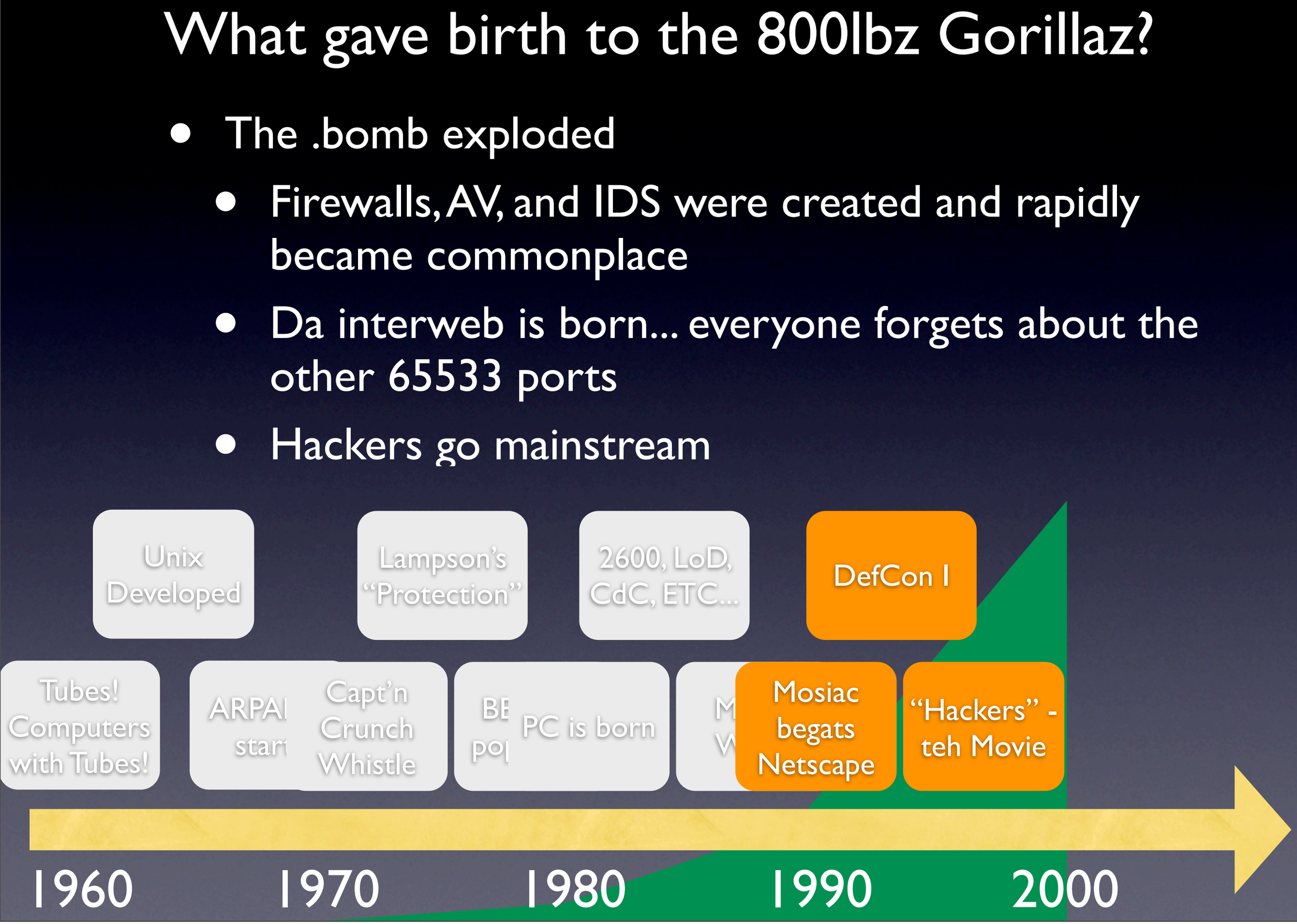
What gave birth to the 800lbz Gorillaz?

- Security emerged as a cottage industry in the 80's
  - BBS's ruled the day
  - Viruses and trojans started going mainstream
  - The hacker underground was born in ernest



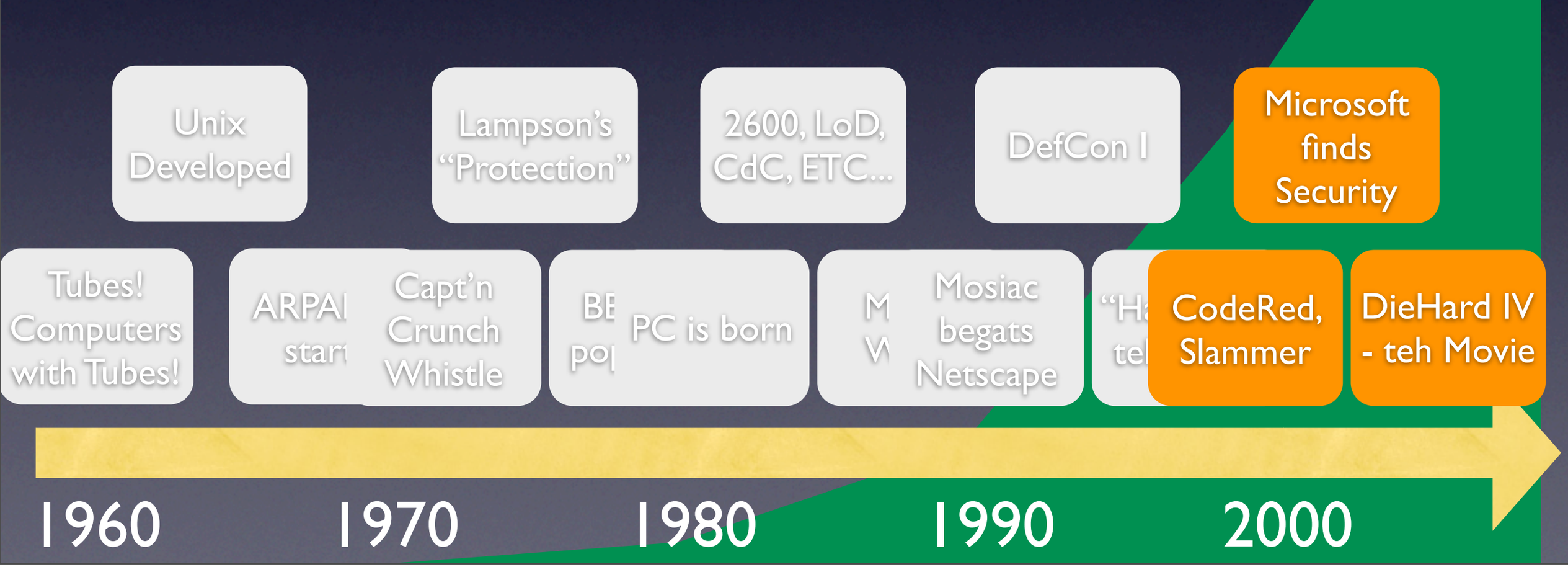
What gave birth to the 800lbz Gorillaz?

- The .bomb exploded
  - Firewalls, AV, and IDS were created and rapidly became commonplace
  - Da interweb is born... everyone forgets about the other 65533 ports
- Hackers go mainstream



What gave birth to the 800lbz Gorillaz?

- The naughties? Social Networking? Oh Noes!
  - The Internet starts its spread everywhere
  - The end of the crypto battle puts strong crypto into everyone's hands
  - Hackers become highly profit driven



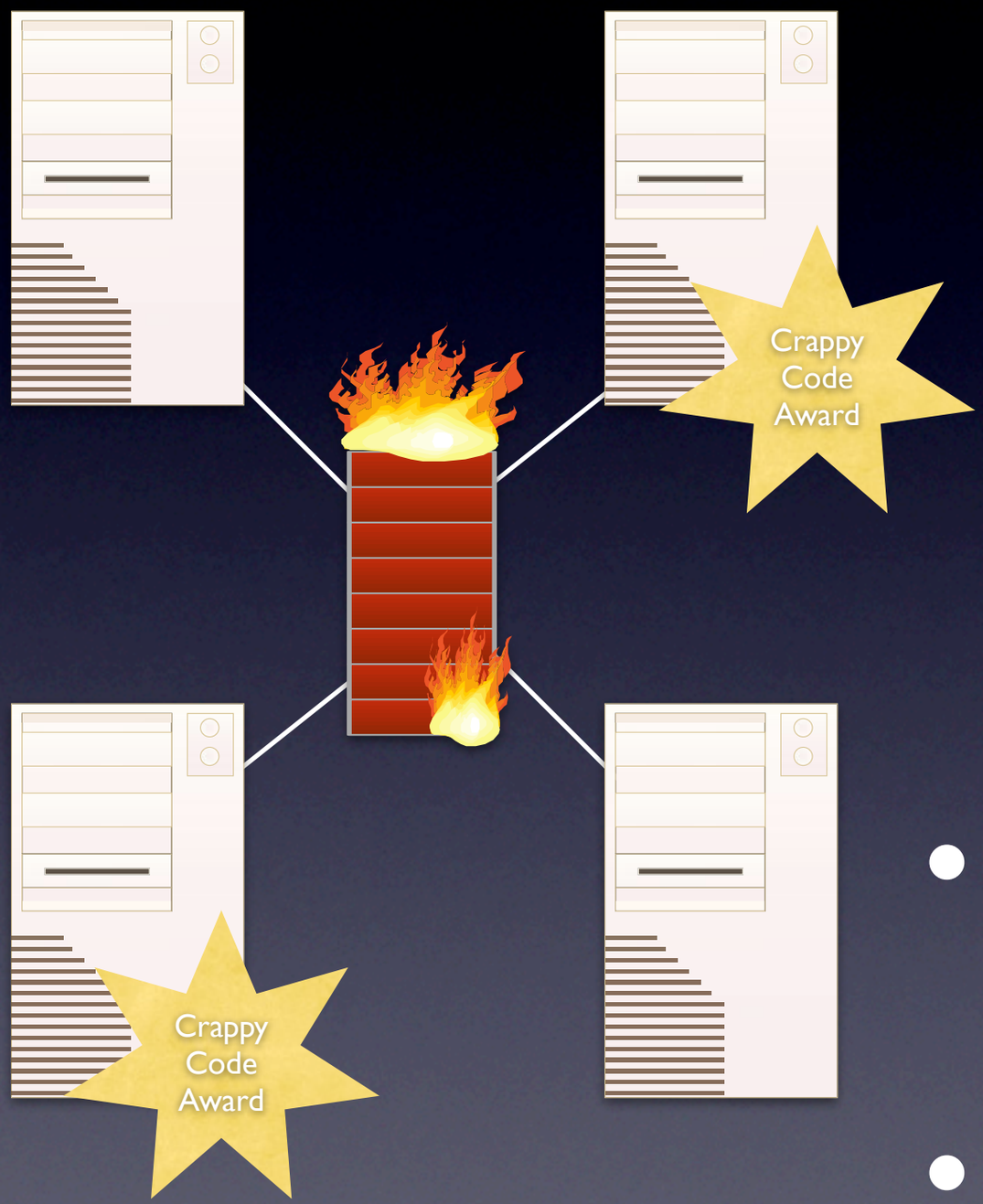
Secret #1 - Defense in Depth is Dead

- In the beginning, there was bad code
  - And there was much rejoicing, because at least we had computers that did stuff for us
- No *type safety*
- No *fault isolation*
- No *error handling*
- No *assurance* in the code
- No real *access control*
- BUT... at least it was doing our bidding

TUBES!

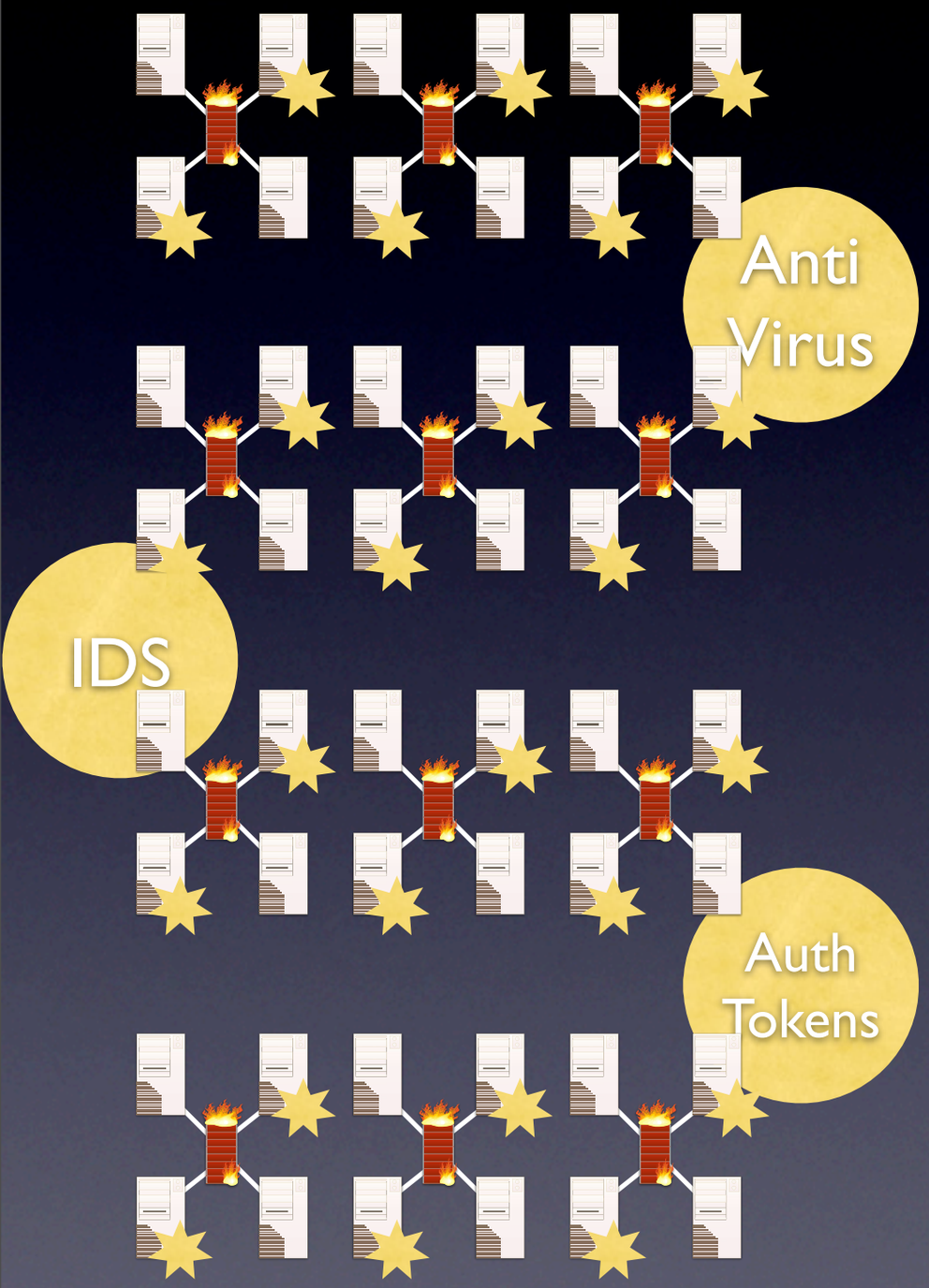


Defense in Depth is Dead



- Over time, we began to network systems together
  - ARPANet, then the Internet
  - Firewalls popped up everywhere
    - TIS released its source
    - Stateful Firewalls
  - But still, we had **bad code**... even more of it than before
- "A firewall is a network response to a software engineering problem" - Steve Bellovin
- The dawn of the firewall age was the beginning of "defense in depth"

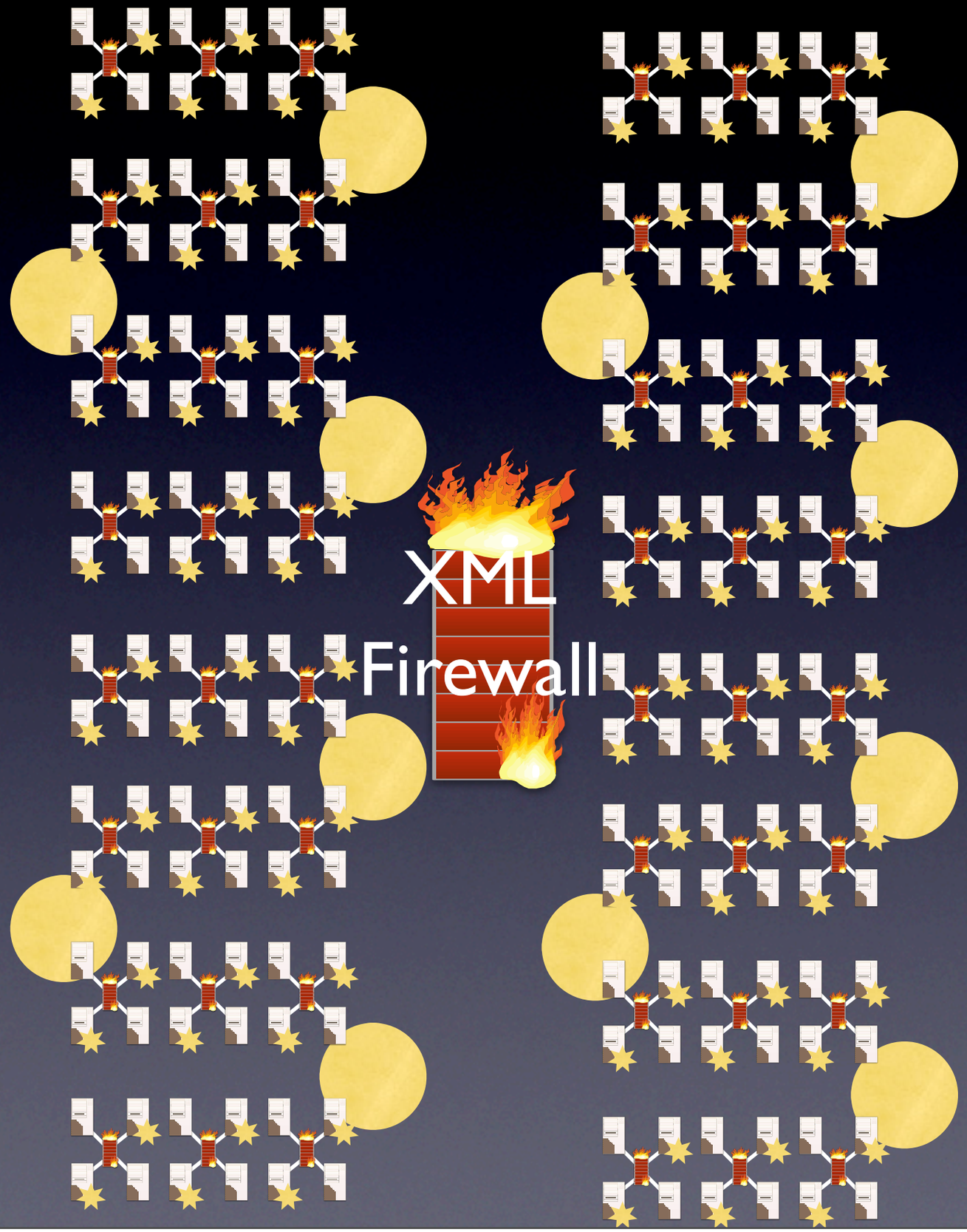
Defense in Depth is Dead



- Then networks became global and attacks started to come in all shapes and sizes
  - So we deployed IDS's, AV, and anti-spam to find the bad guys
  - And we deployed multifactor auth to keep the bad guys out
  - And we spent WAY too much time managing this mess
  - But still we had **bad code**

Defense in Depth is Dead

- Now, we're moving towards service based architectures where the "network is the computer" and SOA rules all
  - So we deploy XML firewalls to protect our applications
  - And we use Single Sign On so our users aren't hassled
- But still we have **bad code**
- All this time, systems have become incredibly complicated
- Millions and millions of lines of code were required for me to type this Power Point slide
- Billions of lines of code define most enterprises



Defense in Depth is Dead

- While KLOC/enterprise has gone through the roof, have we seen a similar increase in power of our security management and operations tools? Have we seen more security staff applied to the problem?
- An idea: Fix the Damn Code!
  - Type safety
  - Secure coding taught to ALL CS majors
  - Trusted computing
- AT LEAST, we need better software controls on our systems, not better firewalls

Secret #2 - We are over a decade away from professionalizing the workforce

- How many people have a degree in anything security related?
  - Most security programs geared towards graduate level students, not the masses of undergrads…
  - And most of those are "Information Assurance", not secure coding, not network security, not security operations
  - How many people here even have graduate degrees?
- The VAST majority of the security workforce has learned how to do their job through self-education, OJT, and (frankly) security conferences and training
  - Name one other USD10Billion industry where the majority of the workforce is basically "untrained" in the eyes of the public and with a zero-level barrier to entry
- So the question remains: How do we codify our knowledge and instruct the next generation of mini-Dans, mini-Halvar's, and mini-DT's?

Looking at the current workforce, we have to realize we can't train everyone

- Software developers are the smartest they'll ever be the day they graduate from college
  - No offense intended…
- Security is everyone's problem, right?
  - Well, you can't train even the people with security in their title, let alone "everyone"
- A single break in the wall usually compromises the entire system... s/a single untrained person/
  - One good work of social engineering can cause huge problems
- Users need tools that don't require education to be used securely

Secret #3 - Many of the security product vendors are about to be at odds with the rest of IT

- This defense in depth thing led to an incredible industry of security products
  - It is estimated the network security market *alone* will be $7bln in a year or two
  - Firewalls, IDS, log analysis, AAA services, etc are a core part of any IT budget
- Very few products are actually geared towards making the foundation more secure
  - Software scanners such as those created by Ounce Labs, Fortify, and Aspect
  - HSM's, smart cards, and other hardware

Secret #3 - At odds

- A recent case study:
  - Microsoft hears the message that consumers want a more secure operating system
  - Microsoft knows that the 64-bit version of the OS is the future and where enterprise demand will be
  - Microsoft integrates driver signing requirements to prevent malicious code from hooking the kernel
  - Security vendors complain that Microsoft is exerting too much control of the kernel and stopping their products from working right
  - Some security vendors (Authentium for instance) find ways to bypass security
  - Microsoft bends and says they'll create API's to allowed some unsigned driver interaction, defeating the purpose of the security mechanism

Secret #3 - At odds

- So, the landscape has shifted
  - The past: *We presumed that the software in our systems was so insecure that we had to buy 3rd party security products*
    - A corollary: *The quality of code in the 3rd party products was worthy of the trust we placed in them*
  - The future: *Software security is a real concern (largely for compliance and legal issues, but whatever) and may big software shops are starting to figure this out*
    - So, what does the future of these 3rd party security products look like?

Secret the Last - Full Disclosure is Dead

- Or at the very least, it's hurt very bad
  - There is tons of money to be had in selling bugs
- Only in the last 15 years has public discussions of Information Security issues come into vogue
  - From obscure geeky bulletin boards to the front page of the NY Times…
- Because of the specialized knowledge required, and the lack of a formal body of knowledge, a community has grown
  - Information on vulnerability research methods, specific vulnerability info and live exploits were publicly discussed
  - The idea of "responsible disclosure" was born (and debated at length)
  - But things have changed…

Decreased exploit development timeframes and mercenary exploit dev are changing the rules

- Patches have two major uses
  - Secure a system that has a known vulnerability
  - Determine what vulnerability was patched in order to develop an exploit
- In the last several years, there has been an incredible decrease in the amount of time between patch release and creation of a successful exploit
  - Microsoft's Patch Tuesday has been great for both attackers and defenders alike
  - The moral? Patch disclosure is essentially the same as vulnerability disclosure
- Many security companies now offer money in exchange for exclusive rights to exploits from mercenary exploit developers
  - Tipping Point's Zero Day Initiative (ZDI)
  - iDefense's Vulnerability Contributor Program (VCP)
  - Many private transactions
- These programs have "rewards" programs, as well as other incentives…

This has TOTALLY changed the "full disclosure" argument

- Changes the foundational argument
  - Previously: What disclosure method should I employ?
  - Now: Should I disclose or should I profit?
    - NOTE: these options *may* not be mutually exclusive, but it's hard to verify its not
- Maybe, just maybe, we've lost track of what we're trying to get done
  - Ultimately, we're trying to make live systems more resilient to attack
  - By creating a secondary market for vulnerability info, we're profiting at (potentially) the expense of the end user

So... where does that leave us?

- The landscape has changed, and we need to recognize it
- We need to push vendors to make products that actually create a secure foundation, not just layer on more protections that need to be managed
- We need to create a more formal body of knowledge for information security... and we need to hold each other accountable

- Now, for some announcements

ShmooCons Past and Future

- ShmooCon 3 was a great success
  - 30 folks helped setup the network via ShmooCon Labs
  - 1000 people showed up... 1000 people left (success!)
  - Raised money for EFF, raised awareness for OLPC
- ShmooCon 4 planning is ongoing
  - Likely dates: Feb 15-17, 2008
  - Likely location: Same. Wardman Park Marriott, DC
  - Likely will continue to be a blast
- Expect some interesting Shmoo announcements in the coming months

w00t!