



Internet Infrastructure Security and Stability

May 12, 2004

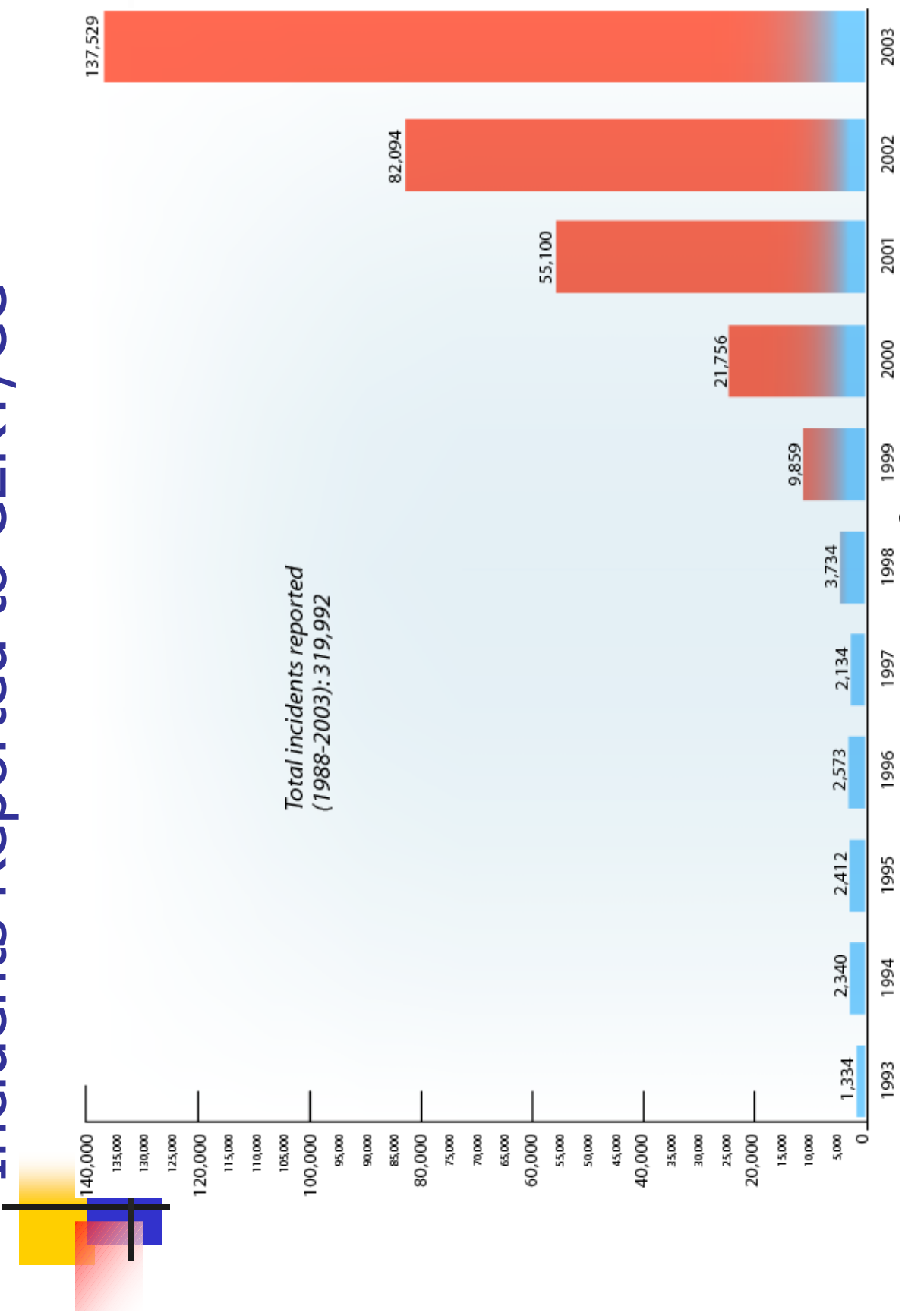
Steve Crocker



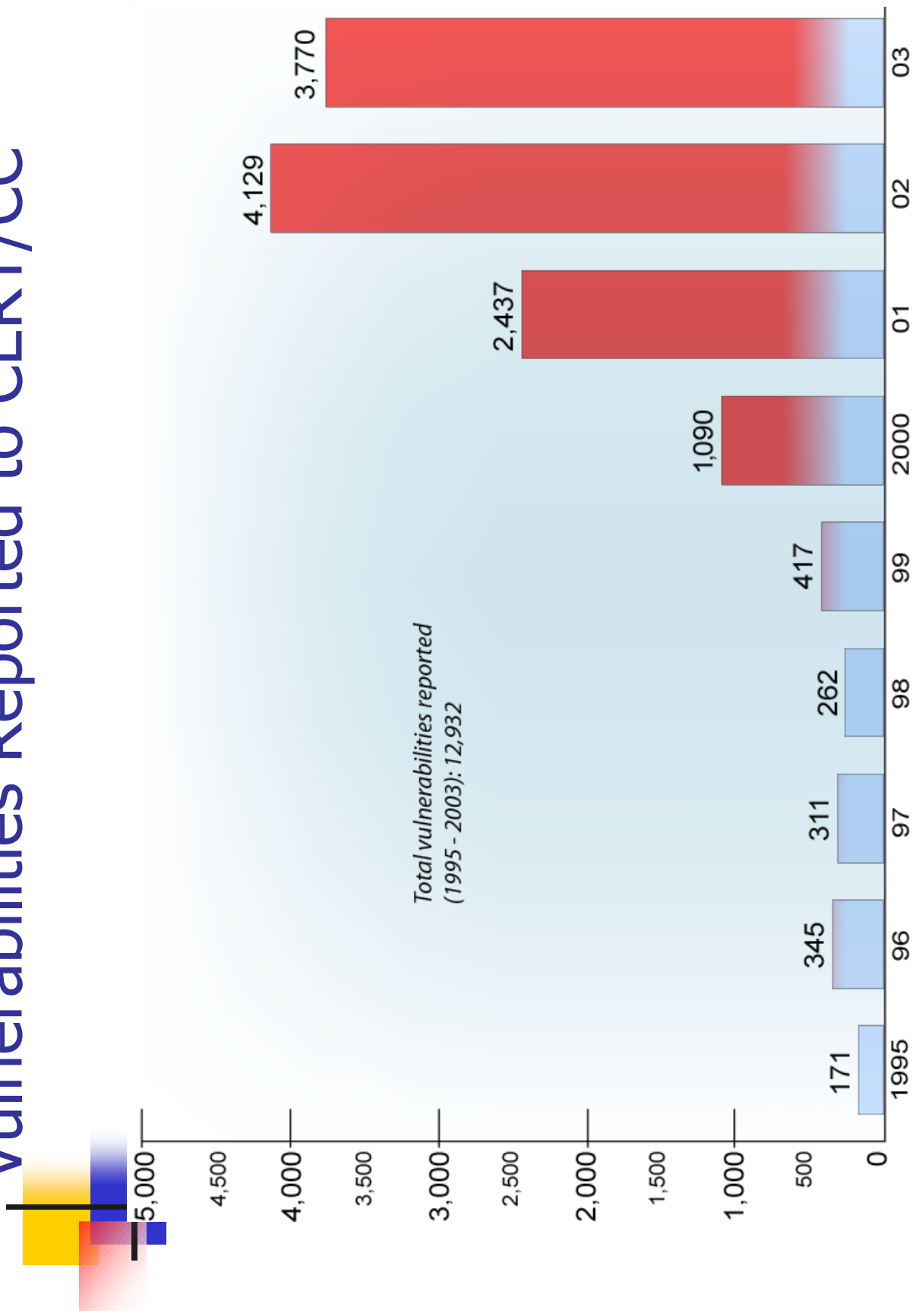
Perspective

- 30 years of involvement with the network
- DARPA Program Manager in the early 70's
- VP Trusted Information Systems
- IETF Security AD in the IETF early 90's
- Chair ICANN's Security and Stability Advisory Committee

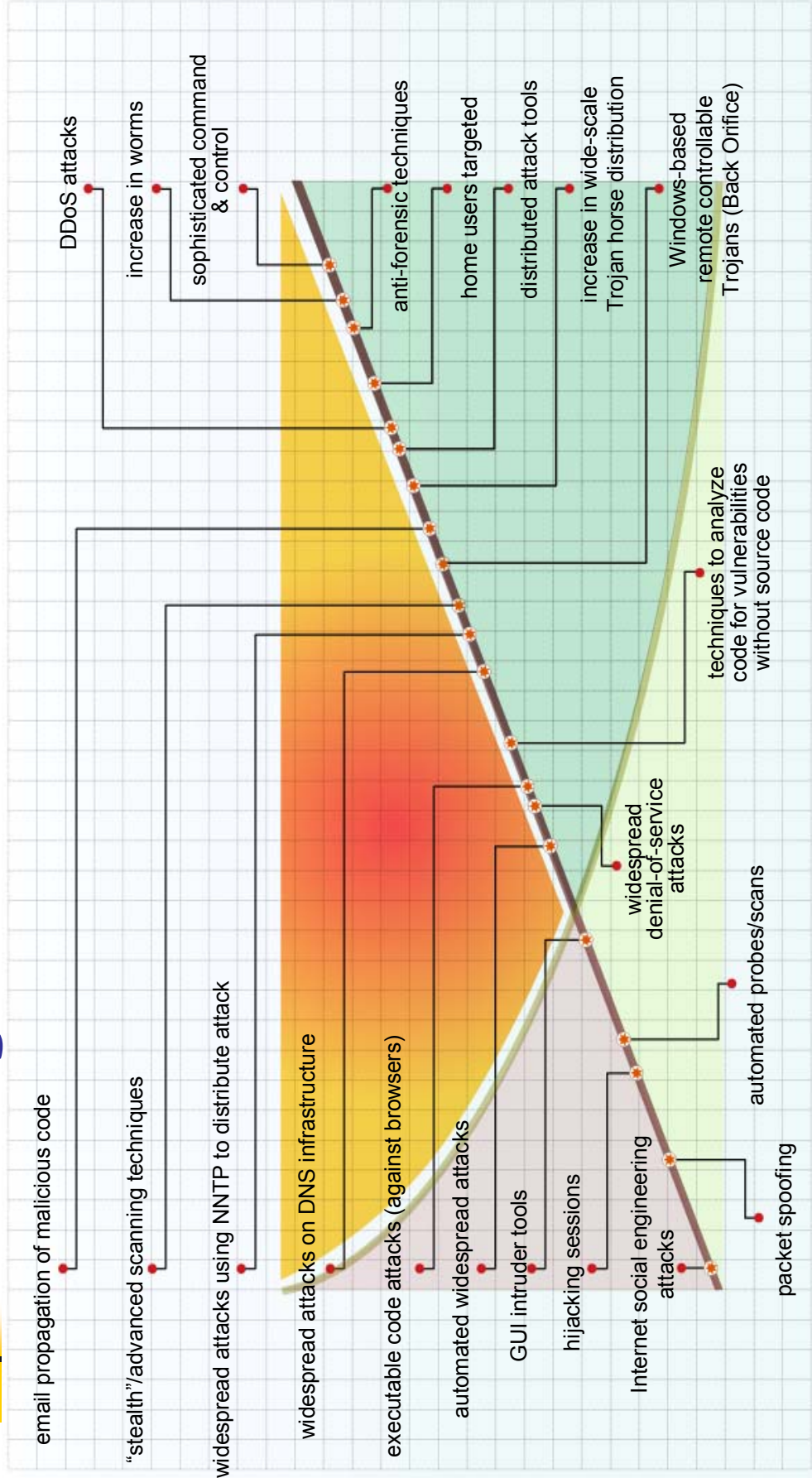
Incidents Reported to CERT/CC



Vulnerabilities Reported to CERT/CC



Attack Sophistication vs. Intruder Knowledge



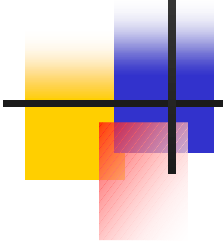
1990

2004



Internet Infrastructure Threats

1. Physical disruption of major lines and switching centers
2. Loss of routing infrastructure continuity and/or fidelity
3. Loss of DNS service continuity and/or fidelity
4. Flooding of network or specific sites, i.e. denial of service attack



DNS Protection

DNS Infrastructure

Root Servers – Status

- Root servers point to Top Level Domains
 - 15 generic TLDs (gTLDs), e.g. .com, .org, etc.
 - US Gov't has .gov and .mil
 - 243 country codes (ccTLDs), e.g. .de, .jp
- Root servers are heavily replicated
 - ~13 independent businesses
 - Many-fold replication and distribution



DNS Infrastructure

Root Servers – Threats

Threats

- **Loss of Service**
 - Network outage
 - Machine or site failures
 - Overwhelming traffic (denial of service attack)
 - Business failure
- **Hijacking**
 - Cache Poisoning
 - False registration
 - Fake zone transfer
 - Fake registrar-registry interaction
 - Private roots
- **Loss of coherence**
 - Unauthorized roots and TLDs
 - Private character set extensions

Countermeasures

- Strong connectivity
 - Distribution, replication
 - Excess capacity
 - DDoS counters (long term)
 - Multiplicity of businesses
-
- Protocol changes, DNSSEC
 - Tight registrar controls
 - TSIG (crypto)
 - Crypto authentication
 - DNSSEC
-
- DNSSEC; policy/political pressure
 - DNSSEC; policy/political pressure

Lots of work underway. This will take more time and money than many expect

DNS Infrastructure

Top Level Domains

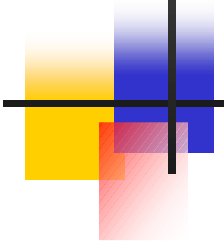


- Similar threats
- One business entity per TLD
 - Some are very robust
 - The big ones are fine, e.g. .com, .org, .jp, .nl
 - Many are very fragile; some will fail
 - This is not a large scale threat; steps are being taken to ameliorate business failures



DNSSEC Status

- 3rd iteration of spec nearing completion
 - Interoperability test found small glitches
 - Will delay final call for IETF spec
- **Several operational and transition issues**
 - Root key management, distribution, rollover
 - End user behavior during long transition
 - Mixture of signed and unsigned zones
 - Incentives for implementation
- **DNSSEC Deployment Forum underway**
 - Open visibility into status of DNSSEC adoption
 - Open dialog on issues, solutions

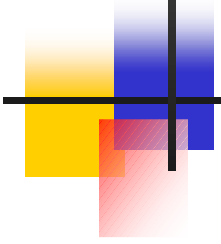


Suppression of Distributed Denial of Service (DDoS) Attacks



The Denial of Service Problem

- Denial of service attacks are increasing
 - This will get worse – probably much worse
- Law enforcement is important but necessarily at the wrong end of the problem
- Technical changes in the Internet would help a lot



A modest(?) proposal for controlling DDos Attacks

- Identify sources of traffic
- Identify “well managed” computers on
“well managed” networks
- Traffic from well managed networks
gets preference



“Well managed”

- “Well managed” computers aren’t zombies
 - Details on the next slide
- Well managed networks quarantine computers which appear to be infected or misbehaving
- Well managed networks report misbehaviors and accept reports of misbehaviors



Weeding out Zombies

- Regular configuration checking
 - Either within the enterprise
 - Or by an outside service
- Tight configuration control
- (Eventually) certified appliances



Network Wide Cooperation

- Traffic among well managed networks gets preference
 - Traffic from same sites is labeled with a “good” bit
 - Eerily similar to Bellovin’s “evil” bit(!)
- When there is congestion, traffic from unmanaged hosts on unmanaged networks is dropped
- How is traffic labeled?
 - IP header bit? MPLS? Other?



DDoS Policy Approaches

- Pressure on the vendor to supply machines that are safe out of the box
- Establishment of an ethic that machines should be safe, i.e. it's the vendor's problem, not the user's.

This all requires R&D, clarity of vision, and perseverance. Not an overnight process.



Arguments in Favor

- Similar to VPN over private lines, but potentially more efficient
- Adds incentive to improve security in hosts and networks
- Raises DDoS protection to a primary goal
- Incremental – works well with a small set of core ISPs and expands smoothly
- Robust – does not require 100% correct operation
 - Failures can be detected; adjustments can be made



Critique

- Sharp shift in policy
- Requires strong cooperation among ISPs
 - Who sets the rules?
- Enforcement issues
 - Who determines when an ISP or a customer isn't complying?
 - What appeals process?
- Efficiency issue for large ISPs: Is it feasible to filter traffic at high speed?