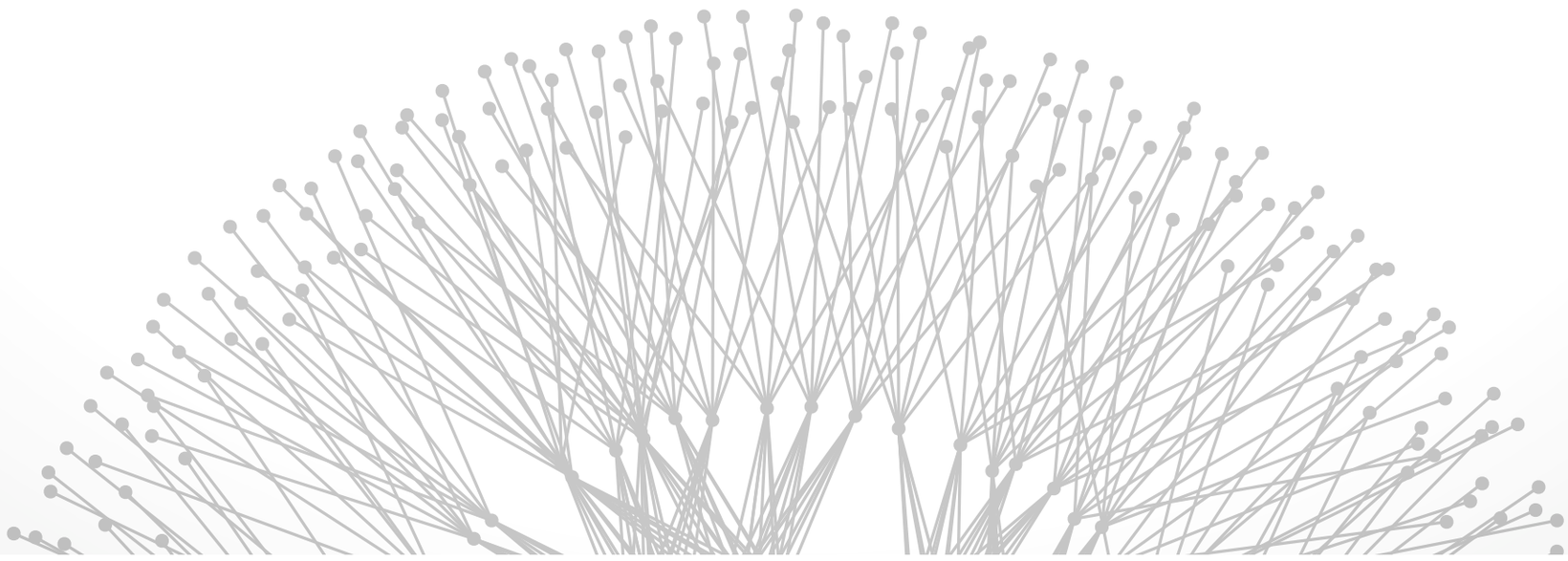
Secure Routing

Brighten Godfrey

CS 538 September 29 2011



Network security

Where was security in the design of the original Internet protocols?

- Virtually nowhere!
- All the core protocols (IP, TCP, DNS, BGP) have trivial, glaring vulnerabilities

When security really matters, rely on end-to-end mechanisms

- Public key cryptography & certificate authorities

With e2e security, what can an attack on BGP still do?

Attacks on Internet routing

Denial of service

- announce "more attractive" path (what does that mean?)
- e.g., more-specific prefix; shorter path; "cheaper" path

Eavesdropping

- like DoS, a kind of traffic attraction
- but somehow get data to destination or impersonate it

Evasion of accountability

- steal someone's prefix or an unused one; send spam; disappear!

How do secure variants of BGP help?

Not just malicious attackers

Many (most) high-profile outages likely just configuration errors

Natural correspondence between attackers and bugs

- behavior unknown ahead of time
- should isolate possible worst-case effects

What about a bug in the protocol?

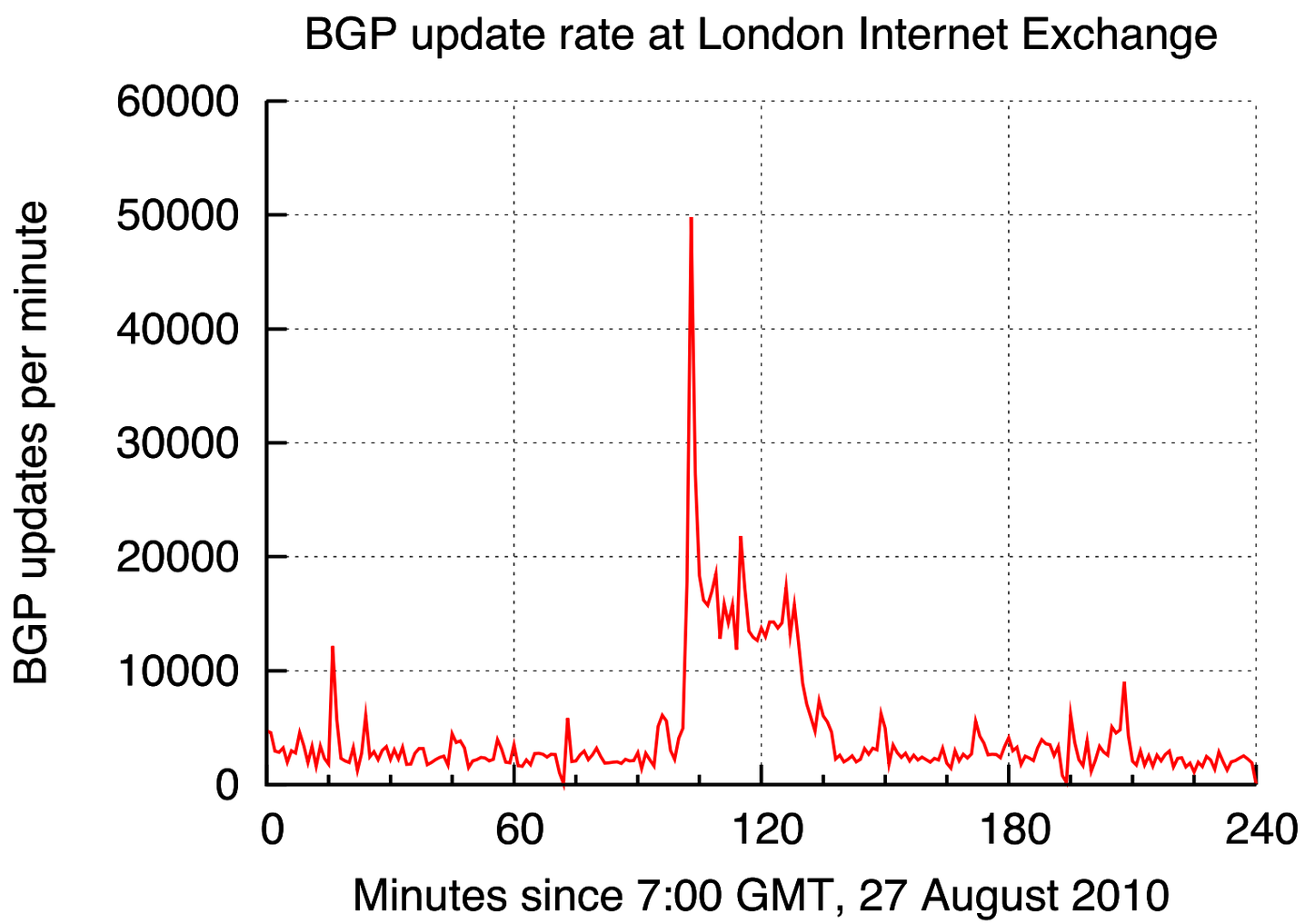
- worst-case scenario: zero-day exploit on large fraction of routers across the entire Internet
- many are running the same software!

A (bad) day in the life of the Internet

About 1% of Internet destinations disrupted for about 30 minutes

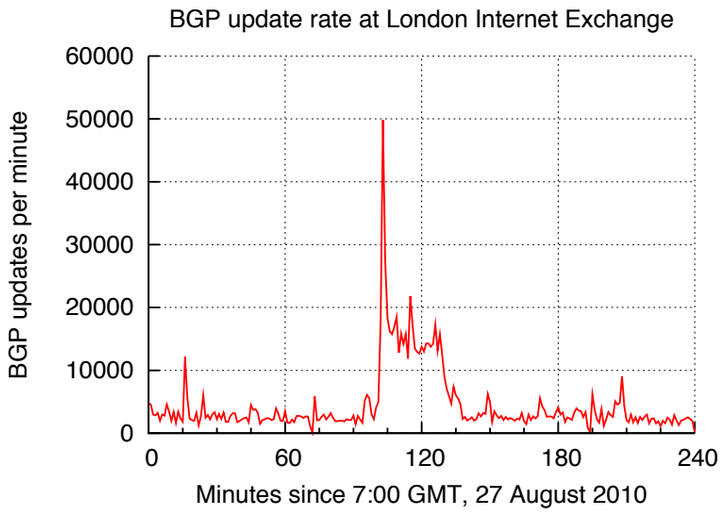
How did this happen?

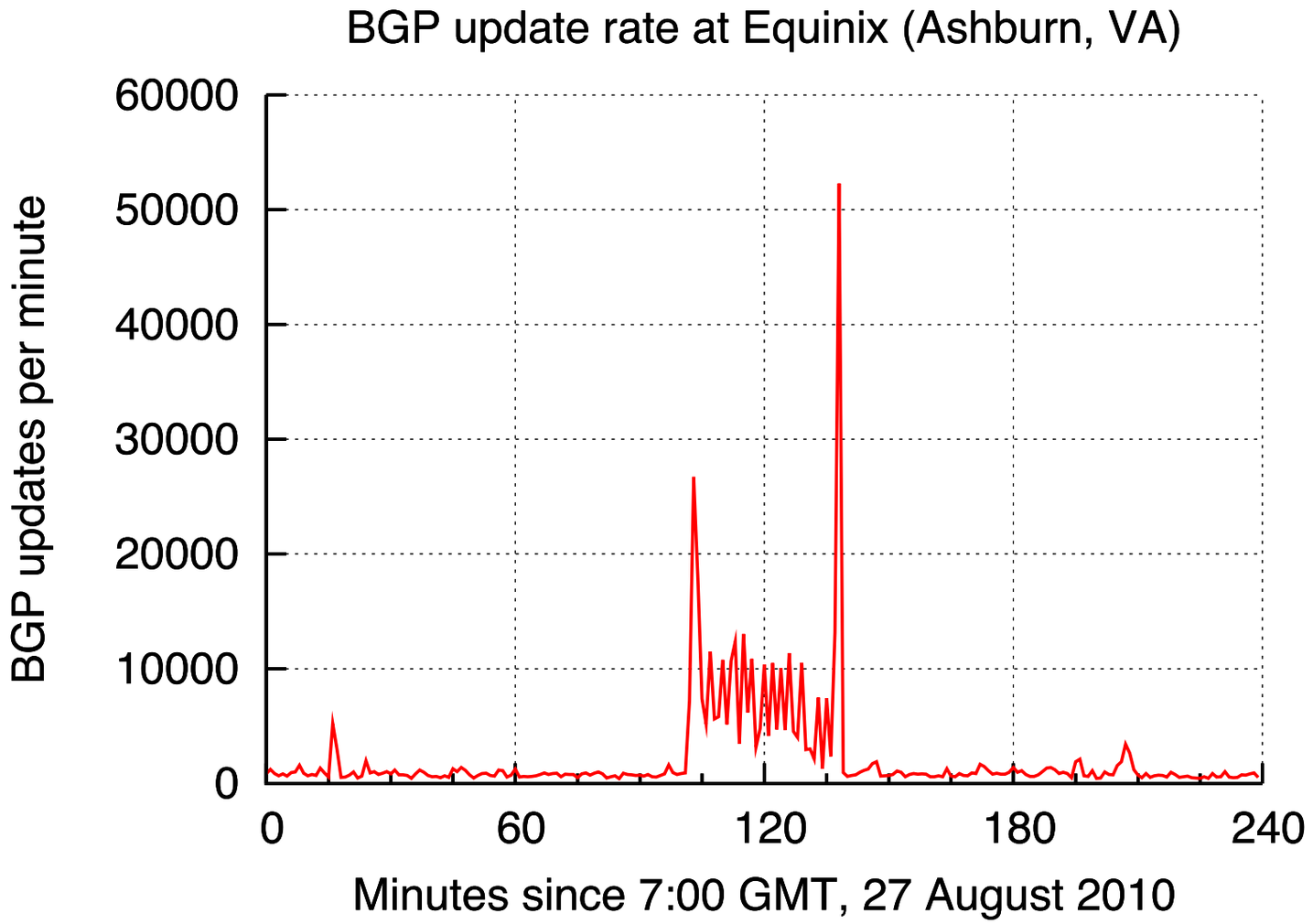
Internet had a bad Friday



[Plots by Brighten based on raw update feeds from Route Views]

Internet had a bad Friday

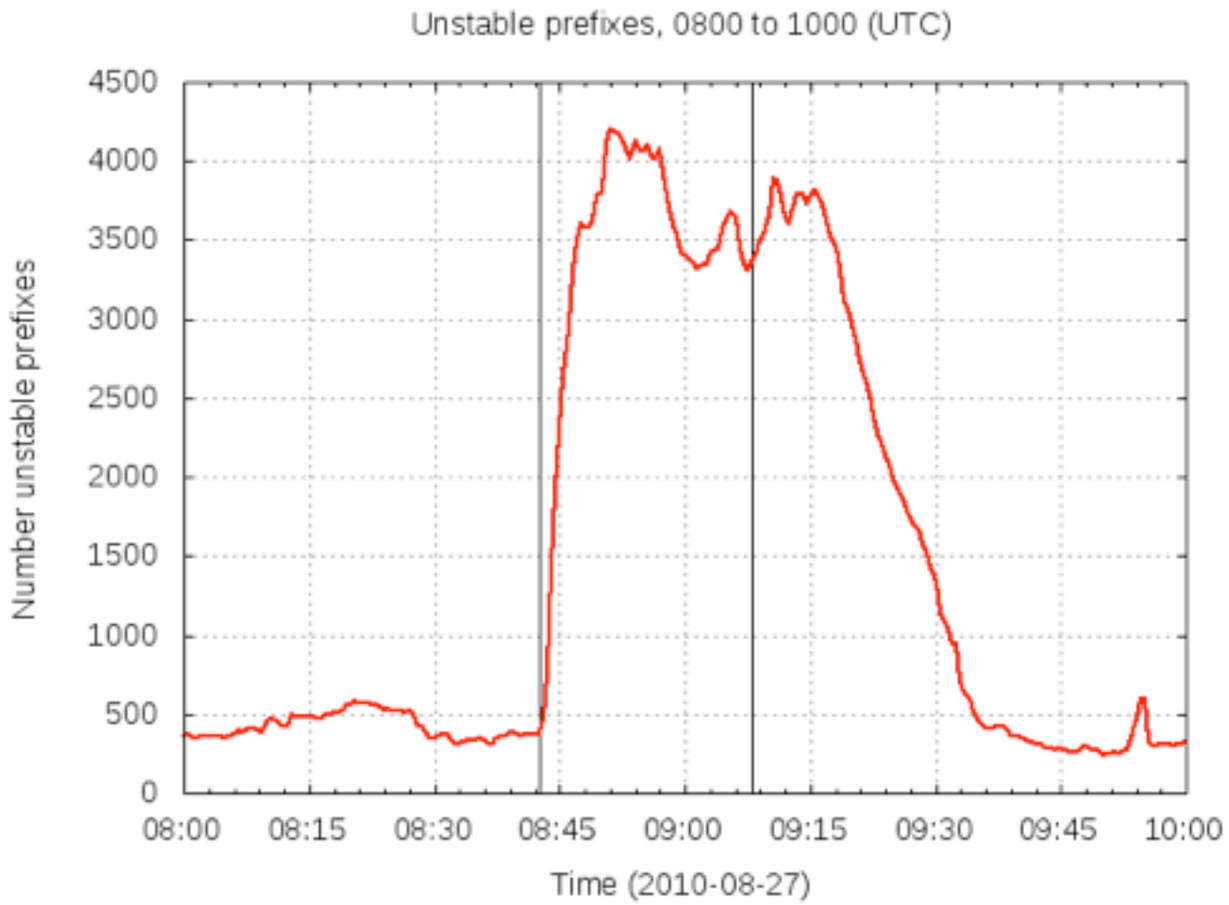


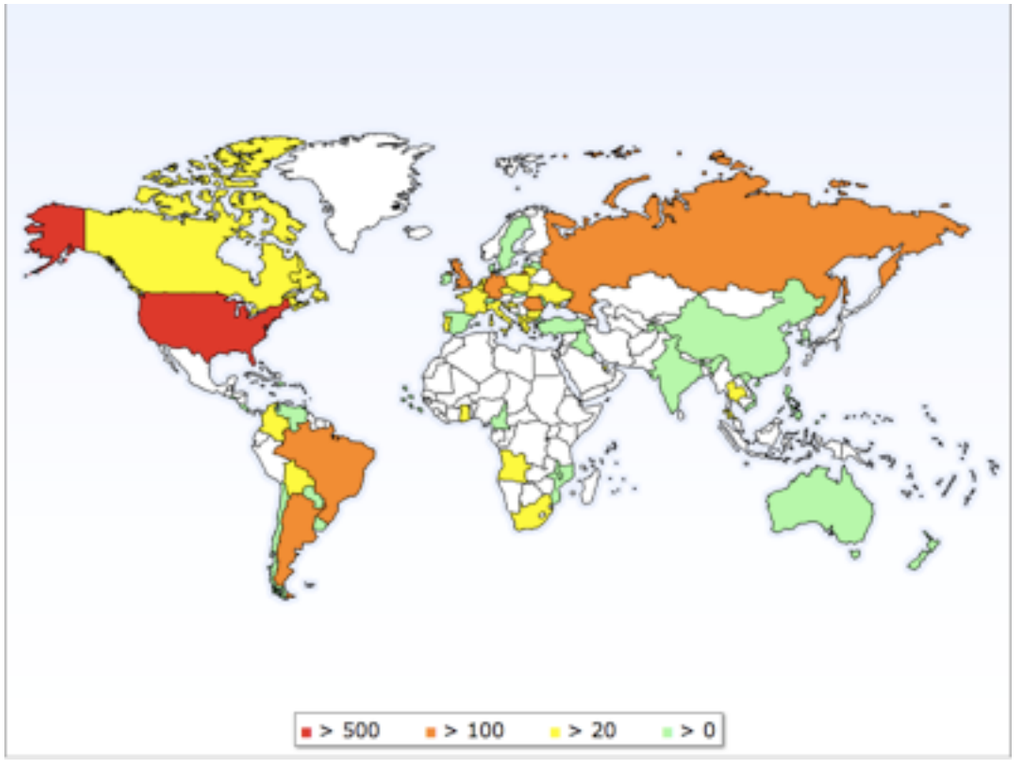


[Plots by Brighten based on raw update feeds from Route Views]

~1% of prefixes affected

[Earl Zmijewski, Renesys]





Brewing a storm

1. An unusual announcement

2. Propagation from router to router

3. Buggy software mangles announcement

4. BGP session dropped upon receipt of mangled message

5. BGP session reestablished and process repeats

Lessons

Many unsavory BGP announcements can be contained, but this one wasn't

- Spread geographically because it was an entirely valid announcement
- Spread to many prefixes because BGP spec lets one bad announcement from a router affect all traffic to that router

Widespread correlated failures from similar software

We're lucky: triggered by researchers, not attackers!