IAB Security Workshop Retrospective

IAB Plenary

IETF 60

Thursday, August 5, 2004

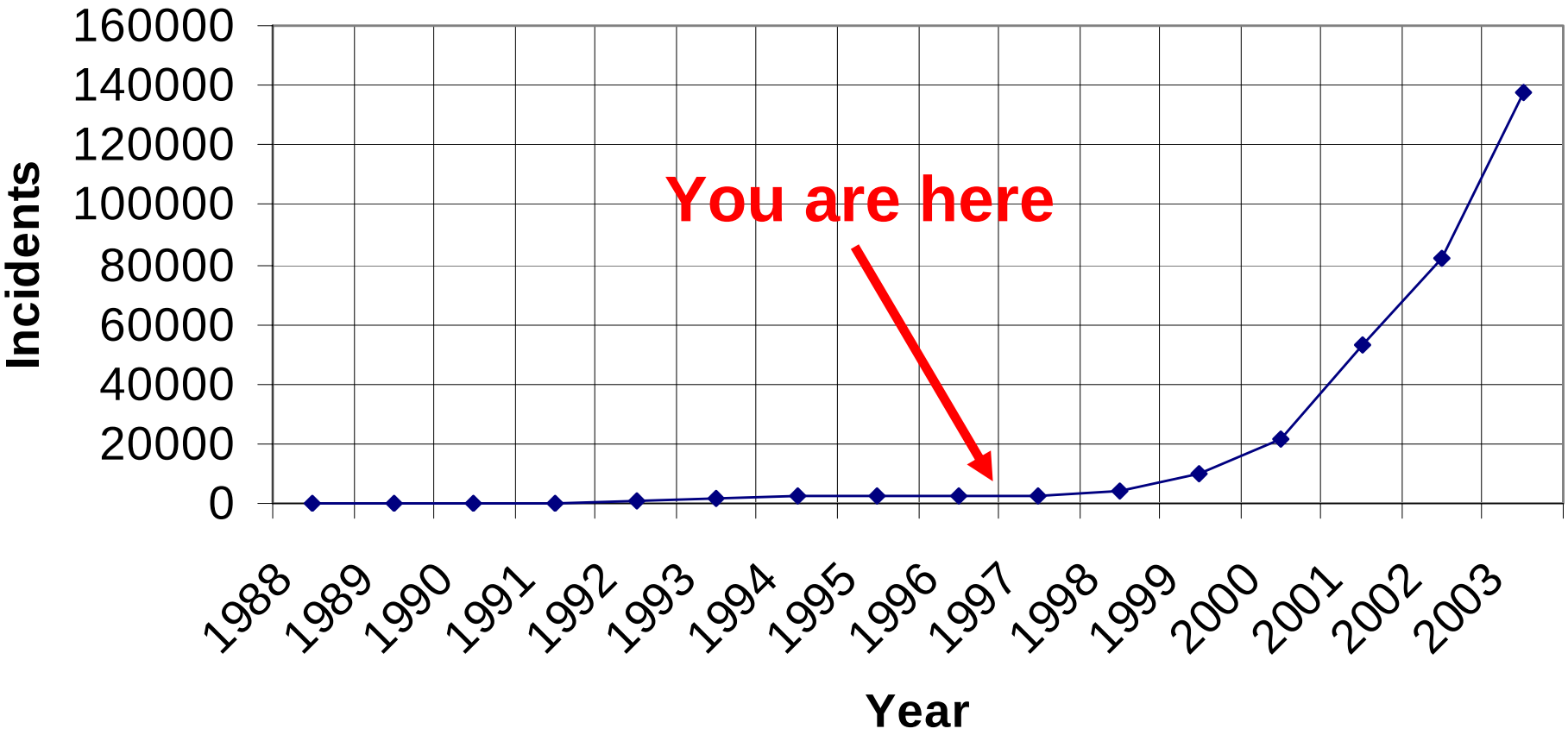
Acknowledgments

- Many thanks to Steve Bellovin for his thoughts and recollections.
- Any errors or omissions are the responsibility of the presenters

RFC 2316 – A Synopsis

- Report of the IAB Security Architecture Workshop
  - Held on March 3-5, 1997 at Bell Labs in Murray Hill, NJ
- Goals
  - To identify the core security components of the Internet architecture
  - To specify documents that needed to be written.
  - To provide useful security guidance to protocol designers.
- Points of agreement
  - Agreed that security was not optional and that it needed to be designed in

1997: The Good Old Days...



What Hasn't Changed

- Trends
  - Rate of attacks is increasing
  - The attackers have gotten smarter
- Several conclusions of RFC 2316 are now common wisdom
  - Security needs to be built in
  - IETF needs to become more serious about security considerations
  - IPsec is not a panacea
  - No cleartext passwords
- Few new security mechanisms

What Has Changed

- Scope and sophistication of attacks has grown dramatically
- ***Money*** now a significant motivation for exploitation of security vulnerabilities
- Increase in peer-to-peer protocol designs vs. client/server
- More multi-party protocols (SIP, AAA, etc.)
- Authorization increasingly important
- Most serious vulnerabilities are now at the application layer
- All this implies an evolution of the threat model

Threat Model Evolution

- Old model: classic communications security threats
- New model
  - Can an attacker make money by exploiting a vulnerability?
    - Via “social engineering”? (phishing)
    - By targeting a high profile user? (blackmail)
  - Can an attacker cause havoc on a regional/national scale?
    - By attacking infrastructure?
    - By denying critical services?

Mechanism Retrospective

- Core
  - DNSSEC not deployed
  - DNS Key RR now deprecated (opponents were right about trust model mismatch)
  - IPsec/ISAKMP not as widely deployed as expected/desired
  - TLS has been widely deployed
  - S/MIME not widely used
    - Though widely *available*
- Not core
  - Kerberos, RADIUS growing in popularity
  - SASL, EAP, GSS-API alive and well (work still ongoing)

Deployment Lessons

- Ease of use a significant consideration
  - SSH, SSL/TLS: easy to deploy
  - SASL, EAP: easy for developers
- Deployment at the edge is easier than in the core
  - Edge: Client VPN
  - Core: Router Security
- Mechanisms requiring coordination are intrinsically more difficult to deploy
  - Examples: PKI, DNSSEC, S/MIME, PGP

Lessons of ISAKMP

- Complexity is the enemy of ease of use
  - How do I explain an SPD to my users?
- General purpose crypto frameworks are hard to design
  - Authorization issues may make it difficult to handle all problems
  - Service definition may differ:
    - Restart vs. Child SAs
    - Machine vs. User Certs
- Will we relearn these lessons with frameworks like GSS-API, EAP, SASL?

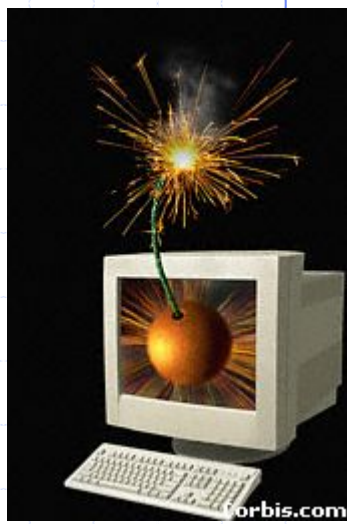
1997: Missing Pieces

- Object security
  - We have the protocols.
  - Usage in specialized applications (e.g. Authenticode)
  - General purpose toolkits are lacking.
- Secure e-mail
  - A demand problem.
  - Requires large scale changes in operations as well as user behavior.
  - Is implementation quality an issue?
- Routing security
  - Some progress here.

2004: Missing Pieces

- Peer-to-peer security mechanisms
- Multi-party protocol security
  - Understanding trust models
  - Breaking the problem into known solvable problems
- DDoS
  - How do we design a protocol that's more DoS resistant?
  - Are there network mechanisms to prevent DDoS?
    - Pushback, etc.
- Phishing
  - Are there authentication mechanisms that will help?

Are We Working on the Right Problems?



- What are the most serious Internet security problems?
  - Spreading malware
  - Zombie networks
    - DDoS
    - Spam
  - Phishing
- All of these are related
  - Its not just the vulnerability of components or individual protocols.
  - It is also their manner of interaction.
  - Looking at components in isolation got us where we are today.
- These issues are not addressed by COMSEC
  - They’re system and software security problems.
- Is the IETF adequately addressing new threats in Security Considerations sections?
  - Communications security threats vs. threats to the life and livelihood of millions

Identifying the Threat Models of Today's Internet

- Look beyond the immediate problem
  - Don't just patch the current bug
  - Does this vulnerability expose other vulnerabilities?
  - Can this fix be used to solve other problems?
- Document your dependencies
  - "This protocol assumes that protocol X functions correctly"
  - Look for cascading failures
- Understand large scale risks
  - The Internet is increasingly critical infrastructure
  - Monetary incentives can overcome difficulties in exploiting vulnerabilities
  - Epidemics spread fast, and develop immunity to countermeasures

Feedback?