Lessons from the Internet

Fred Baker

Important lessons from the Internet

- The service is **connectivity**
- **Scaling** is critical
- **Simplicity** is the watchword; elegance and re-usability are keys to both scaling and innovation
- **Robust Interoperability** is more important than mere correctness

The service is connectivity

- While we measure connectivity in terms of round trip time, throughput, and the usability of favored applications, *the fundamental service of the Internet is the ability to send a datagram from an arbitrary system to any other system within the limits of applicable policy*.

The current exponential growth of the network seems to show that **connectivity is its own reward**, and is more valuable than any individual application such as mail or the World-Wide Web. This connectivity requires technical cooperation between service providers, and flourishes in the increasingly liberal and competitive commercial telecommunications environment.

RFC 1958 http://www.ietf.org/rfc/rfc1958.txt

The ability to scale is critical

- In the Internet, regardless of the domain an application, protocol, or technology is designed for, if it is at all useful it quickly finds itself crossing arbitrary distances and in use by vast numbers of systems.
- A technology, protocol, or application that scales super-linearly - and often one that merely scales linearly - becomes untenable very quickly.

Mike O'Dell

Corollaries on scaling

- Saltzer's *End to End Principle*,

  “Functions placed at low levels of a system may be redundant or of little value when compared with the cost of providing them at that low level”

  Saltzer, Reed, and Clark: End to end arguments in system design, 1984

- *Amplification Principle*

  “Local optimizations should have only local effect”

  Meyer and Bush, RFC 3439

- *Coupling Principle*

  “Periodicity should be randomized”

  Meyer and Bush, RFC 3439

Simplicity is the watchword; elegance and re-usability are keys to both scaling and innovation

- "The *Simplicity Principle*… states that complexity is the primary mechanism which impedes efficient scaling, and as a result is the primary driver of increases in both capital expenditures (CAPEX) and operational expenditures (OPEX). The implication for carrier IP networks then, is that to be successful we must drive our architectures and designs toward the simplest possible solutions."

Meyer and Bush, quoting Mike O'Dell

RFC 3439 http://www.ietf.org/rfc/rfc3439.txt

Robust Interoperability is more important than mere correctness

- The *Robustness Principle*

  "Be conservative in what you do, be liberal in what you accept from others",

  More familiarly stated in the words of religious leaders and philosophers throughout time and geography: "do to others as you would have them do to you"

- Many systems, and many Internet implementations, have ignored the rule to their own peril.

  It is not sufficient to do the specified thing when the rules are clear; it is necessary to do a reasonable thing that is likely to have a beneficial result when under duress.

Jon Postel

RFC 793 http://www.ietf.org/rfc/rfc0793.txt

Corollary security principle

Principle of Least Privilege

- Component variant

  Communications network components and operating system APIs must have access only to functions, ports, protocols, and services that are necessary for the performance of their duties, with all other access prohibited.

  This includes grid devices, general purpose clients and servers, and network elements.

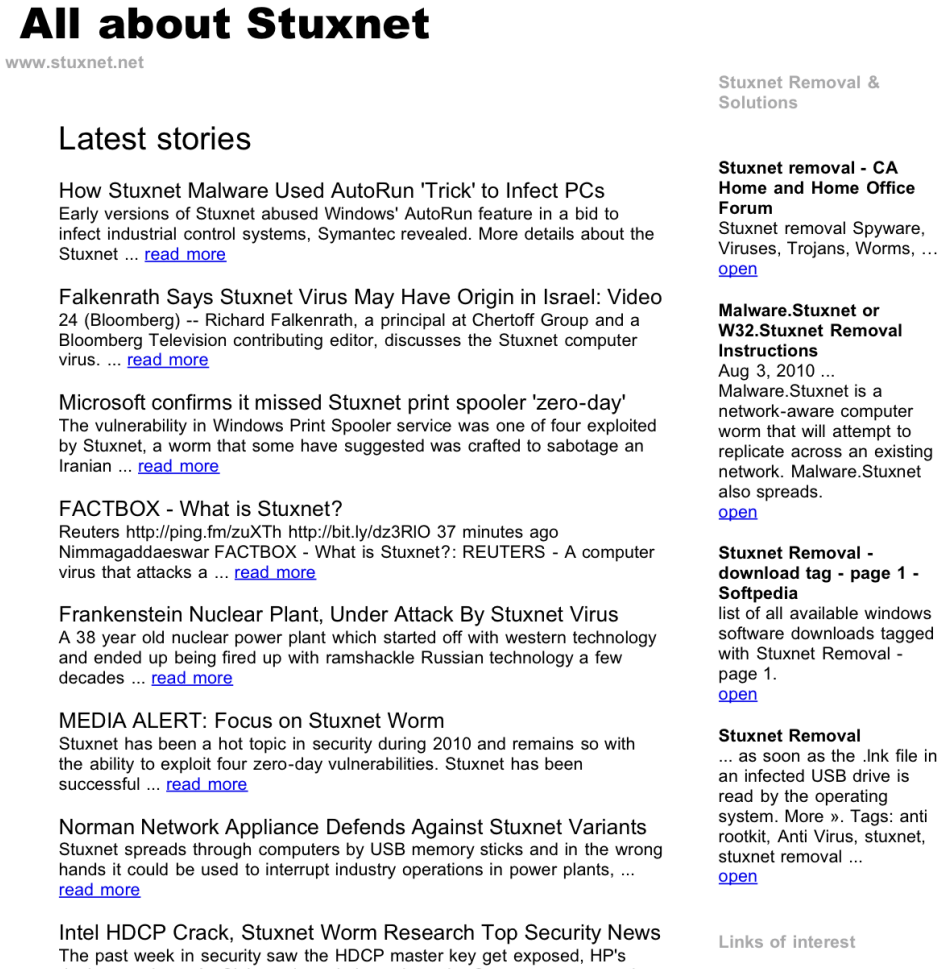
- User variant

  Users (common users and administrators) only have access to systems and portions of network components and grid devices needed in the performance of their duties

NISTIR 7628 Volume 1, SG.AC-7 and SG.CM-7

Example of an attack: Stuxnet

- Said to be military-grade weapon that attacks specific control systems
  - Detected June 2010
  - *Depends on disabling automated processes in process control systems*
- Not carried by the Internet
  - But obviously could be
  - Therefore prototypical weapon of motivated attacker
- Worst way to defeat it:
  - Security by obscurity
- Best way to defeat it:
  - *Not get the virus*
  - *Not execute the code*



All about Stuxnet

www.stuxnet.net

Latest stories

How Stuxnet Malware Used AutoRun 'Trick' to Infect PCs
Early versions of Stuxnet abused Windows' AutoRun feature in a bid to infect industrial control systems, Symantec revealed. More details about the Stuxnet ... read more

Falkenrath Says Stuxnet Virus May Have Origin in Israel: Video
24 (Bloomberg) -- Richard Falkenrath, a principal at Chertoff Group and a Bloomberg Television contributing editor, discusses the Stuxnet computer virus. ... read more

Microsoft confirms it missed Stuxnet print spooler 'zero-day'
The vulnerability in Windows Print Spooler service was one of four exploited by Stuxnet, a worm that some have suggested was crafted to sabotage an Iranian ... read more

FACTBOX - What is Stuxnet?
Reuters http://ping.fm/zuXTh http://bit.ly/dz3RIO 37 minutes ago Nimmagaddaeswar FACTBOX - What is Stuxnet?: REUTERS - A computer virus that attacks a ... read more

Frankenstein Nuclear Plant, Under Attack By Stuxnet Virus
A 38 year old nuclear power plant which started off with western technology and ended up being fired up with ramshackle Russian technology a few decades ... read more

MEDIA ALERT: Focus on Stuxnet Worm
Stuxnet has been a hot topic in security during 2010 and remains so with the ability to exploit four zero-day vulnerabilities. Stuxnet has been successful ... read more

Norman Network Appliance Defends Against Stuxnet Variants
Stuxnet spreads through computers by USB memory sticks and in the wrong hands it could be used to interrupt industry operations in power plants, ... read more

Intel HDCP Crack, Stuxnet Worm Research Top Security News
The past week in security saw the HDCP master key get exposed, HP's deal to purchase ArcSight and revelations about the Stuxnet worm targeting industrial ... read more

Stuxnet Removal & Solutions

Stuxnet removal - CA Home and Home Office Forum
Stuxnet removal Spyware, Viruses, Trojans, Worms, … open

Malware.Stuxnet or W32.Stuxnet Removal Instructions
Aug 3, 2010 ... Malware.Stuxnet is a network-aware computer worm that will attempt to replicate across an existing network. Malware.Stuxnet also spreads. open

Stuxnet Removal - download tag - page 1 - Softpedia
list of all available windows software downloads tagged with Stuxnet Removal - page 1. open

Stuxnet Removal
... as soon as the .lnk file in an infected USB drive is read by the operating system. More ». Tags: anti rootkit, Anti Virus, stuxnet, stuxnet removal ... open

Links of interest

What kinds of security mechanisms?

Communication Layer	Type of control	Example
Data Content	End to end integrity in message-based exchange	W3C XML Signature
Application Layer	Application to application authentication, authorization, encryption	TLS, HTTPS, DKIM, S/MIME, SSH
Network Layer	System-to-system authentication, authorization, encryption	IPsec ESP
Physical/Link Layer	Limited Membership	Protected SSID, IEEE 802.1X with EAP-TLS

Pick one

Internet Community to Smart Grid: adopt our working technologies; *make new mistakes*

- Focus on security

  We have defined and partially implemented security solutions, but many don't use them

  Use them

- Addressing

  We have largely used up the IPv4 address space;

  Use the larger address space in IPv6

- Focus on interoperable manageability

  We have solutions for this, but little market requirements;

  Use proven encodings like XML and application architectures like BEEP, ATOM, and XMPP

Lessons from the Internet

Fred Baker

