DoS-resistant Internet Working Group (WG)

Registry of Attacks & Defences

Martin Koyabe
BT Group CTO

menu

Pt I

- WG – Registry task contribution
  - What we are focusing on

menu

Pt I

Pt II

- WG – Registry task contribution
  - What we are focusing on
- Taxonomy of attacks and defences
  - Our plans & related work
  - First stab - multi-attribute (e.g. based on attack phases, types etc)
  - Open discussion (for more ideas)

BT

menu

Pt I

- WG – Registry task contribution
  - What we are focusing on
- Taxonomy of attacks and defences
  - Our plans & related work
  - First stab - multi-attribute (e.g. based on attack phases, types etc)
  - Open discussion (for more ideas)

Pt II

- Managing input for this task
  - Attack registry – members only (access after given period)
  - Defences registry – strictly members only (layered access)
  - Who will be responsible ?

Pt III

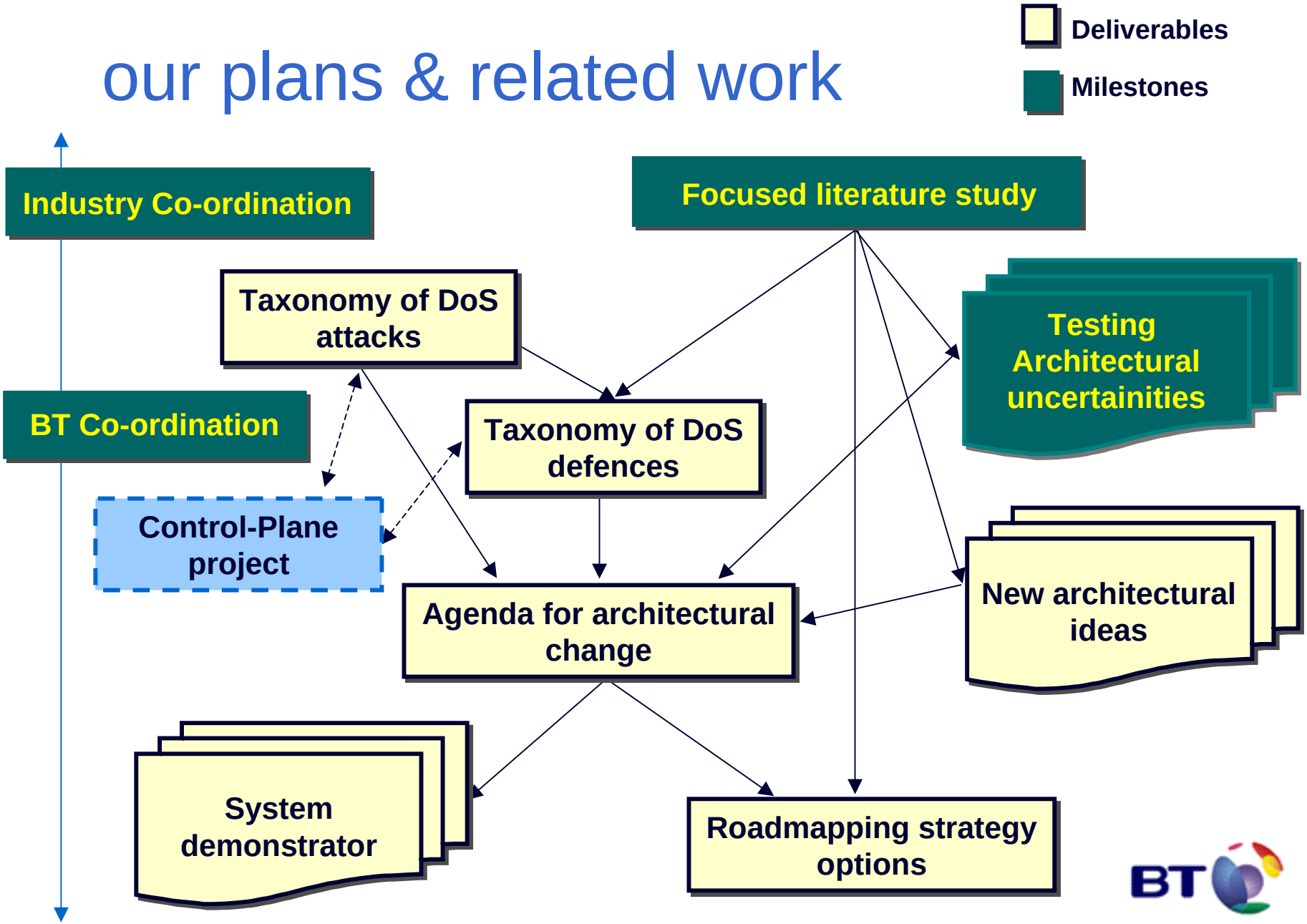
BT

wg-registry task progress - focus

- Registry of attacks
  - End-host attacks (e.g. CPU, memory exhaustion)
  - Infrastructure attacks (e.g. bandwidth exhaustion, CPU cycles)
  - Possible attacks & motivation issues (much broader scope)
- Registry of defence
  - Based on securing the core network (neighbour authentication)
  - Incidence response techniques
    - Detection – manual (netflow count) or automatic (Arbor peak flow)
    - Traceback – Non-spoofed or Spoofed IP address
    - Containment – ACL, sinkholing/re-direction, Scrubbers
  - New architectural defences

BT

our plans & related work



a stab at taxonomy – challenges [1/2]

- Some points on why DoS attacks are possible today ?
  - Difficult to stop DoS attack at the receiver
    - » one party misbehaves, hurts the other
  - Internet security interdependent
    - » attacks from compromised hosts
  - Accountability not enforced
    - » attackers use spoofed IP addresses to perpetrate attacks
  - Control is distributed
    - » Internet management distributed, global control difficult

BT

a stab at taxonomy – challenges [2/2]

- Some challenges on DoS defence today ?
  - Need for distributed response on the Internet
    - » global distribution & co-ordination of responses is challenging
  - Economic and social factors
    - » parties that do not suffer attacks may be reluctant to join in
  - Lack of detailed attack information
    - » publicly reported attacks might damage business reputation
  - Lack of defence system benchmarks
    - » Lack of reputable benchmark suite of attack scenarios
  - Difficulty of large-scale testing
    - » DoS defenses need to be tested in a realistic environment

BT

a stab at taxonomy of attacks [1/2]

- Characterise by transition phases
  - **recruit**, **exploit**, **infect** and **use** phases
  - Differentiate between *manual*, *semi-automatic* and *automatic*
- Characterise by end-host, infrastructure & other
  - End-systems (PCs, Network server)
    - » resource and memory exhaustion
  - Infrastructure Routers
    - » routing protocols, forwarding
  - DNS, links, firewalls & IDS systems
  - Physical DoS
  - Social engineering
  - Legal

BT

a stab at taxonomy of attacks [2/2]

- Characterise by bandwidth or resource depletion
  - Bandwidth depletion
    - » Flood attacks, amplification attacks
  - Resource (memory) depletion
    - » Protocol exploit attacks, malformed pkt attacks
  - Processor depletion

BT

a stab at taxonomy of defences

- Characterise by defence type
  - » Whether its preventive or reactive
  - » How it operates - autonomous, co-operative or interdependent
  - » Deployment location – victim, intermediate or source network
- Characterise by countermeasures
  - » whether it detects and neutralise handlers (IRC etc)
  - » Whether it detects/prevents secondary victims
  - » Whether it mitigates and stops attacks
  - » Whether it deflects attacks (honey pots etc)
  - » Whether it does post-attack forensic

BT

managing input for the task

- Known Volunteers
  - Malcolm Hutty (LINX) – Create a Wiki for the group
  - Julian Rose (Atlas)
- Grey areas to be sorted out..
  - Access to attacks registry
    - » All members should have access (need to agree !!)
    - » Make it public after a set period (n Months, n = 6, 12 etc)
  - Access to defence registry
    - » Strictly members only, never published
    - » Needs structured restriction

BT