Challenges and Tolerance
Outline

- Motivation
- Past failures
- Challenge model and taxonomy
- Challenge tolerance
Challenges and Tolerance

Motivation

• Motivation
• Past failures
• Challenge model and taxonomy
• Challenge tolerance
Resilience
Motivation: Reliance

- Increasing reliance on network infrastructure
  - consumers
  - commerce & financial
  - government and military

⇒ Increasingly severe consequences of disruption
⇒ Increasing attractiveness as target from bad guys
Resilience
Motivation: Consequences

• Increasing reliance on network infrastructure
⇒ Increasingly severe consequences of disruption
  - threat to life and quality of life
  - threat to financial health economic stability
  - threat to national and global security
⇒ Increasing attractiveness as target from bad guys
Resilience

Motivation: Attractiveness

• Increasing reliance on network infrastructure
  ⇒ Increasingly severe consequences of disruption
  ⇒ Increasing attractiveness as target from bad guys
    – recreational and professional crackers
    – industrial espionage and sabotage
    – terrorists and information warfare
Resilience
Definition

- Resilience
  - provide and maintain acceptable service
  - in the face of faults and challenges to normal operation

- Challenges
  - large-scale disasters
  - socio-political and economical challenges
  - dependent failures
  - human errors
  - malicious attacks from intelligent adversaries
  - unusual but legitimate traffic
  - environmental challenges
Scope of Resilience
Relationship to Other Disciplines

Challenge Tolerance
- Survivability
  - many \( \lor \) targeted failures
- Fault Tolerance
  - few \( \land \) random
- Traffic Tolerance
  - legitimate, flash crowd
  - attack, DDoS
- Disruption Tolerance
  - environmental
    - delay, mobility, connectivity
  - energy

Robustness Complexity

Trustworthiness
- Dependability
  - reliability, maintainability, safety
- Availability
- Integrity
- Security
  - confidentiality, nonrepudiability
  - auditability, authorisability, authenticity
- Performability
  - QoS measures

Fault Tolerance
- (few \( \land \) random) ∨ (many \( \lor \) targeted failures)

Fault Tolerance
- legitimate, flash crowd
- attack, DDoS

Traffic Tolerance
- energy

Dependability
- reliability
- maintainability
- safety

Fault Tolerance
- (few \( \land \) random) ∨ (many \( \lor \) targeted failures)

Security
- confidentiality
- nonrepudiability
- auditability
- authorisability
- authenticity

Performability
- QoS measures
Challenges and Tolerance

Past Failures

- Motivation
- Past failures
- Challenge model and taxonomy
- Challenge tolerance
Resilient Networks
Sub-Disciplines: Challenge Tolerance

• Survivability against attack and large-scale disasters
  – tolerate many and correlated failures
  – fault tolerance: tolerate one (or several) random failures
    • subset of survivability sub-discipline

• Traffic tolerance
  – DDoS attacks
  – legitimate traffic such as flash crowds

• Disruption tolerance
  – tolerate environmental challenges
  – mobility, weak/episodic connectivity, long delay
  – energy constraints
Resilient Networks
Sub-Disciplines: Challenge Tolerance

- Survivability
  - many ∨ targeted failures

- Fault Tolerance
  - few ∧ random

- Traffic Tolerance
  - legitimate flash crowd
  - attack DDoS

- Disruption Tolerance
  - environmental delay
  - mobility connectivity
  - energy

- Trustworthiness
  - Dependability
    - reliability maintainability safety
  - availability integrity
  - confidentiality nonrepudiability
  - auditability authorisability
  - authenticity

- Security
  - AAA
  - authentication
  - auditability

- Performability
  - QoS measures

- Availability integrity

- Fault Tolerance
  - legitimacy flash crowd attack DDoS

- Disruption Tolerance
  - environmental delay mobility connectivity energy

- Survivability
  - many ∨ targeted failures

- Traffic Tolerance
  - legitimate flash crowd attack DDoS

- Trustworthiness
  - Dependability reliability maintainability safety
  - availability integrity
  - confidentiality nonrepudiability
  - auditability authorisability
  - authenticity

- Security
  - AAA authentication auditability

- Performability
  - QoS measures
**Survivability**

**Definitions**

- **Survivability**
  - capability of a system to fulfill mission in a timely manner
  - in presence of large-scale natural disasters, attacks, failures

- **Challenges**
  - disasters
    - natural
    - human-made
  - challenges to Internet waist
  - social, political, economical factors
Disasters

Natural Disasters

• Terrestrial
  – earthquake, tsunami
• Meteorological
  – hurricane, thunder and rain storm, derecho, ice storm
• Cosmological
  – geomagnetic storm
Hengchun Earthquake
Overview

• 26 Dec. 2006: 7.1 Earthquake south of Taiwan
• Seven of nine cable in Luzon strait severed
  - severe disruption to Internet services in Asia
    • spike of almost 4000 ASes for 2 hours
    • ~1200 ASes out for much longer
  - ~40% disruption to international telephony
  - greatest impact in Taiwan and Hong Kong
• Significant impact
  - some local Asian traffic rerouted across Pacific Ocean
• 14 Feb. 2007: All cables repaired
Hengchun Earthquake Lessons

- Many Asian cables share geographic fate
- Redundancy without diversity is not resilient
- Routing algorithms & policy should anticipate failures
Hurricane Katrina Timeline

- 2005 hurricane Katrina timeline
  - Storm surge potential devastation to NO well understood
    - including Oct. 2004 National Geographic article
  - 23 Aug 17:00 EDT TD 12 announced
  - 24 Aug 11:00 EDT upgraded to TS Katrina
  - 25 Aug 17:00 EDT upgraded to hurricane cat 1
  - 25 Aug 18:30 EDT 1st landfall Dade/Broward FL
  - 26 Aug 01:00 EDT downgraded to tropical storm
  - 26 Aug 05:00 EDT upgraded to cat 1 hurricane
  - 26 Aug LA gov declares emergency
  - 26 Aug 23:00 EDT NHC forecasts landfall at Buras LA
Hurricane Katrina Timeline

- **2005 hurricane Katrina timeline**
  - 27 Aug 05:00 EDT  upgraded to cat 3
  - 27 Aug  NO mayor orders voluntary evac
  - 27 Aug  LA gov asks fed disaster decl.
    - including NO and Jefferson Parish
  - 27 Aug  US pres declares disaster for LA
  - 27 Aug  FEMA issues disaster order
    - does not include NO or Jefferson Parish
  - 27 Aug  NHC briefs pres, LAgov, NO mayor
  - 28 Aug 12:40 CDT  upgraded to cat 4
  - 28 Aug 07:00 CDT  upgraded to cat 5
Hurricane Katrina Timeline

- **2005 hurricane Katrina timeline**
  - 27–28  NO surge inundation predicted
    - Weather Channel, Wunderground, etc.
  - 28 Aug 11:01 CDT NWS predicts devastating damage:
    - major structural failure; uninhabitable for weeks
    - power outages lasting for weeks
  - 28 Aug  mandatory NO evacuation ordered
  - 28 Aug  pres issues disaster for AL, MS, FL
  - 28 Aug  LA gov requests Nat. Guard
    - (but not authorised until 1 Sep)
  - 29 Aug 06:10 CDT landfall near Buras and NO
Hurricane Katrina Timeline

- 2005 hurricane Katrina timeline
  - 29 Aug 08:00 CDT flooding reported Industrial Canal
  - 29 Aug 14:00 CDT NO confirms 17th St. Levee breach
  - 29 Aug FEMA director discourages outside help
  - 30 Aug 60–80% of NO under water
  - 30 Aug pres announces task force to meet 31 Aug
  - 30 Aug DHS sec. decl. Incident Nat. Significance
  - 31 Aug first relief supplies to NO Superdome
  - 31 Aug BNSF and NS restore most rail service
Hurricane Katrina
Timeline

• 2005 hurricane Katrina timeline

  - 01 Sep aft  CNN broadcasts from conv. center
    • drove in on Crescent City Connection (Bus. US-90)
  - 01 Sep eve  DHS sec dismisses con. ctr. as rumor
  - 01 Sep      Gretna LA seals Bus. US-90 with force
Hurricane Katrina
Infrastructure Relationships

• Power grid fails
  - lines downed by trees/wind; facilities flooded
    • 2.6M w/o power
    • NO power out for a month
  - restoration crews unavailable
    • still in FL
    • lack food, water, shelter

• Communication and network infrastructure
  - insufficient battery and generator backup
  - backup not robust (time duration and spatial diversity)
[http://www.oe.netl.doe.gov/hurricanes_emer/katrina.aspx]
Hurricane Katrina
Emergency Communications Impact

• Incompatible communications
  - NO 1992 M/A-Com
  - LA 1996 Motorola
  - multiple incompatible federal systems
  - MS national guard used sneakernet

• NO communication not survivable
  - Energy Center tower lost power
  - backup power transformer taken out by glass shard
  - MA-Com repair crews denied entry for 3 days by state police

• Amateur radio again critical
Hurricane Katrina
PSTN Impact

• 1.3 million Bellsouth customers out

• Most cellular telephone service fails
  – cell towers have insufficient battery backup
  – remaining network severely overloaded
  – wireless operators
    • refuse to release data on outages
    • claim network is robust – regulation for backup life not needed
      – regulation proposed after 9/11

• Few satellite phones
  – many with dead batteries
Hurricane Katrina
Internet Impact

• Little impact on national Internet service
• Significant impact on local Internet service

Hurricane Katrina Failures

- **Disaster preparedness**
  - long-term planning and infrastructure deployment
    - brittle power grid: lines above ground, facilities floodable
    - non interoperable first-responder infrastructure
    - brittle network infrastructure
  - short-term planning
    - insufficient preparation for storm

- **Response**
  - long-term planning for rapid deployment
    - almost non-existent
  - short-term response
    - insufficient equipment staging for response
Geomagnetic Storms
Overview

• Due to CME (coronal mass ejection) or solar flares
• Impacts
  – space communication: GPS and other satellite systems
  – radio signals: first observed in 1847 in UK telegraph
  – submarine cables: observed in 1958
• Most notable:
  – 1989, Canada: 9 hours of power blackout
Disasters

Human-made Disasters

- EMP attack
- Space debris due to collision of satellites
- Fires
- Cable cuts
- Pandemic
- Power blackouts
- Human errors
EMP Attack
Overview

- EMP (electromagnetic pulse) weapons:
  - wide-scale impact ~ 1500 km
  - malicious and deliberate
- Impact primarily on:
  - wireless communication
  - power systems
- Recovery from such attack can take months
Hinsdale Central Office Fire

Overview

- 08 May 1988: Hinsdale Illinois Bell central office fire
  - building catches fire during electrical storm
  - switching equipment and cables completely destroyed

- Impact
  - 100K customers lose service for *weeks*
  - also major disruptions in
    - long distance
    - 800
    - 911
    - cellular
    - ATC for O’Hare
Hinsdale Central Office Fire Lessons

- Fault tolerance not sufficient
  - SS7 network redundant, but redundant components burned
- Resilience requires
  - spatially diverse redundancy
  - separation of infrastructures
Baltimore Tunnel Fire
Overview

• 18 July 2001: Howard St. CSX rail tunnel fire
  – train derails in tunnel
  – tripropylene tank car catches fire
  – other cars catch fire, including paper and wood materials
  – HCl tank car ruptures
• Fire burns for 5 days
• Impact
  – parts of downtown Baltimore closed for several days
  – rail traffic disrupted
  – multiple fiber optic cables melted
    • WorldCom set up alternate links in 36 hours
Baltimore Tunnel Fire
Lessons

• Plan for vulnerabilities
  – threat was predictable

• Redundancy without diversity not survivable
  – dual homing to service providers sharing tunnel
Mideast Submarine Cable Cuts
Overview

• 30 Jan. 2008: two Mediterranean cables severed
  – north of Alexandria Egypt
  – significant disruptions to Algeria, Egypt, Sudan, Lebanon, Syria, Saudi Arabia, UAE, Pakistan, India, Maldives, Bangladesh
  – ~70% of Egyptian and Pakistani ASes down

• 19 Dec. 2008: three Mediterranean cables severed
  – south of Palermo Italy
  – significant disruptions to Egypt, Sudan, Saudi Arabia, Maldives, Sri Lanka, Bangladesh
  – ~80% of Egyptian ASes down

[http://research.dyn.com/2008/01/mediterranean_cable_break]
[http://research.dyn.com/2008/12/deja-vu-all-over-again-cables]
Mideast Submarine Cable Cuts

Map

Mideast Submarine Cable Cuts

Cause

• Cause undetermined
  – no evidence of terrorism

• Cable cuts frequent
  – dragging anchors, friction against rock

• Relatively few Mideast routes
  – Mediterranean ↔ Suez ↔ Red Sea
Mideast Submarine Cable Cuts

Lessons

• Mideast has limited cable service
  – geographically concentrated
• Redundancy without diversity is not resilient
H1N1 Influenza Pandemic
Overview

- Mar. 2009: Outbreak detected in Mexico
- Apr. 2009: WHO declares health emergency
- Jun. 2009: WHO declares pandemic
  - due to global spread
  - but cases are generally mild
- Oct. 2009: first vaccines become available
H1N1 Influenza Pandemic

Risks

• Too early to tell if H1N1 will have major impact
  - but the potential is severe
• Many organizations do not have pandemic plan
  - economic incentive for employees to come in sick
• Potential disruptions to network if humans sick
  - on which health care and information delivery rely
NE Power Failure

Overview

• 265 power plants with 508 generating units offline
• ~10M without power
  - OH, MI
  - PA, NY
  - QC
NE Power Failure Impact
Myths vs. Ground Truth

- NASA images ➔
- Urban legends ↓

NE Power Failure
Official US + Canada Causes

• Official causes
  - inadequate system understanding
  - inadequate situational awareness
  - inadequate tree trimming
    • three 345kV 3phase lines downed 14 Aug 2003 15:05–15:32
  - inadequate RC (reliability coordinator) diagnostic support

• Blaster & other worms did not have “significant” role
  - CERT, RCMP, NCS joint study

NE Power Failure
Official US + Canada Recommendations

• Official recommendations
  - implementation of mandatory reliability standards
  - strengthening North American Electric Reliability Council
  - develop independent NERC regulator funding mechanism
  - address specific deficiencies (FirstEnergy & reliability orgs)
  - strengthen NERC technical recommendations
  - improving training and certification requirements
  - increasing the physical and cyber security of the network
NE Power Failure
Lessons and Risks

• Lessons: power grid very brittle
  - SCADA systems inadequate
    • control and monitoring
  - operators poorly prepared and trained
  - overall architecture of grid?

• Risks
  - SCADA system insecure
    • security by obscurity doesn't deter serious attackers
  - share fate with Internet
    • back-end interconnection provides back door
      - Slammer took down Davis-Besse nuke monitoring in Jan 2003
    • common links subject to congestion and DDOS
Disasters
Challenges to Internet Waist

- Internet hourglass model reflects architecture
- Minimally required element: IP
- BGP and DNS bloats narrow waist
- Globally impacting events observed
- BGP originally deployed in 1989
  - BGP-4 deployed in 1993
- Since then 15 major BGP hijacks
  - BGP hijacking: prefix is advertised by some AS
Pakistan YouTube Hijack

Overview

• 24 Feb. 2008: Pakistan Telecom hijacks YouTube
  – in response to order from Pakistan Telecom Authority

• AS17447 advertises part of AS36561 (YouTube)
  – 208.65.153.0/24 advertised by Pakistan Telecom
  – 208.65.152.0/22 allocated to YouTube
  – packets go to more specific advertised prefix

• YouTube responds
  – advertises more specific /25 prefixes

• PT withdraws advertisement ~2 hours later
  – having suffered the wrath of network operators worldwide

[http://research.dyn.com/2008/02/pakistan-hijacks-youtube-1]
Pakistan YouTube Hijack Lessons

• Trust models work only when trusted parties behave
  - PT permitted to send AS advertisements
  - but is expected to not advertise others prefixes

• Other serious but accidental failures
  - 1997: MAI propagates full Internet prefix announcement
  - 2005: TTnet Turkey advertises entire Internet
  - 2006: Con Ed advertises prefixes of others
Challenges to DNS

Overview

- DNS used for 32 bit address to name mapping
- Built on hierarchy
- Challenges to DNS includes:
  - misconfigurations
  - attacks
- DNS attacks can be categorized:
  - cache poisoning
  - DDoS attacks against root name servers
    - 2002 against root servers
    - 2006 against top level domain servers
  - domain name hijacking
Disasters

Social, Political, Economical Factors

- Terrorist attacks
- Political unrest
- Depeering
- Net neutrality
- Censorship
- Privacy
9/11 Terrorist Attacks

Overview

• 11 Sep. 2001: terrorists fly planes into WTC towers
  – WTC 1, 2, and 7 collapse

• Collapse causes significant infrastructure damage but localized to lower Manhattan
  – power outages
  – communications infrastructure
9/11 Terrorist Attacks
Lessons

• Significant disaster but in very localized area
• Non-interoperable first-responder communications
• Mobile telephony
  – not sufficiently over-provisioned for emergency load
  – not sufficiently over-provisioned to absorb wireline traffic
  – unreasonable reliance for first-responder backup
• Internet effects very limited due to localization
  – flash crowd effects on news servers
7/7 Terrorist Attacks

Overview

• 07 Jul. 2005: Terrorist attack on London Transport
  - three bombs on the Underground; one on a bus
• Little impact to networking *infrastructure*
• Significant impact from network traffic
  - mobile telephony saturated
  - Vodafone enables ACCOLC to prioritize emergency calls
    • ACCOLC: Access Overload Control
7/7 Terrorist Attacks

Lessons

• Significant events can overload networks
  - networks not provisioned for catastrophic events
  - but some provisions can be made to prioritize
Arab Spring Repression
Overview

• 2010 Arab spring
  - revolutionary actions to depose dictators and autocracies
  - revolutions in Tunisia, Egypt, Libya
  - ongoing uprisings in Syria, Libya, Yemen
  - protests in Algeria, Iraq, Jordan, Kuwait, Morocco, Oman, …

• Internet and mobile networks role
  - social media (Facebook and Twitter) heavily used
  - organizational activities and news reporting

• Many governments have disabled network
  - shut down Web servers and IP routers
  - disabled mobile PSTN facilities
Arab Spring Repression
Lessons

- Internet levels power to people
- conventional survivability can be subverted by governments
Peering Disputes
Overview

• Peering: agreement to exchange traffic between ISPs
  - settlement-free: no payments
  - both parties must agree that one-another benefit
  - generally done among ISPs with similar traffic exchange

• Disagreements may arise
  - one partner decides that the other should pay for transit
  - if one partner depeers, traffic is no longer exchanged
  - customers cannot reach one-another
    • unless multi-homed to other providers not in dispute
Cogent Peering Disputes

Overview

• Cogent involved in many peering disputes
  - 2003: AOL
  - 2006: France Telecom
  - 2005: Level 3: particularly nasty disagreement
  - 2008: TeliaSonera: customers disconnected for 2 weeks
  - 2008: Sprint-Nextel: claimed no peering agreement existed
Peering Disputes

Lessons

• Network ops depends on *nontechnical* factors
  - policy
  - economics
  - regulation

• Can result in significant network disruptions
Net Neutrality
Overview

• Economically motivated
  – ISPs wanting to charge for more $

• Two ideas around it:
  – proponents: QoS, traffic management, financial gains
  – opponents: against open nature of Internet

• Important cases:
  – 2008: Comcast vs. BitTorrent

• What’s the sole purpose of networking?
Censorship Overview

- Politically or economically motivated
- Censorship mechanisms:
  - IP address filtering
  - URL keyword filtering
  - DNS redirection
- Canonical example: Great Firewall of China
  - almost every nation has some sort of filtering
    http://map.opennet.net/
- Usually local impact
  - Chinese I-root name server misconfiguration; global impact
Privacy
Overview

• Privacy: authorized communication between parties
• CALEA for voice approved in 1994
  – Communications Assistance for Law Enforcement Act
• CALEA for VoIP approved in 2004
• Community raised flag (EFF, scholars, etc.)
  – deep packet inspection required for IP packets
  – concerns
    • against end-to-end principles
    • what if technology is used by malicious parties?
Traffic Tolerance
Overview

• Ability to withstand abnormal traffic conditions

• Traffic anomalies due to:
  - flash crowds:
    • sudden event due to simultaneous multiple requests
    • observed in 9/11 and 7/7 primarily on telephone networks
    • objects modified on CNN.com website, additional Akamai CDNs
  - DDoS attacks:
    • CERT and NIST provides databases
Information Warfare

Objective

- Information warfare with different objectives:
- Military-oriented
  - in 2008 DoD networks penetrated (agent.btz worm)
    - counter operation: Operation Buckshot Yankee
    - USB ports epoxied shut in DoD
- Economic (industrial) espionage
  - more than DDoS attack, it is about *protection of data*
- Techno-terrorism (by governments or organizations)
  - Titan Rain 2005
  - Estonia 2007
  - Stuxnet 2010
International Information Warfare

Example Cases

• 2005 Titan Rain attacks
  - most likely by Chinese military against US defense networks

• 2007 Estonian DDoS attack
  - DDoS attack against government and financial Web servers
  - motivated in part by Tallinn statue relocation and
  - Estonia accused Russia of helping

• 2010 Stuxnet worm
  - MS Window vector to attack Siemens control software
  - targeted Iranian nuclear enrichment centrifuges

• Ongoing Anonymous attacks
  - formed 2003; began series of DDoS & cracking attacks 2008
  - e.g. against RIAA and MPAA after MegaUpload seizure
State-sponsored Traffic Engineering

Iran Elections

- Elections took place on 12 June 2009
- Iran DCI traffic reduced from 5 Gb/s to 1 Gb/s
- Application traffic blocked
- Proxy servers used to overcome filtering

Traffic Tolerance

Lessons

• Internet and its components vulnerable
  – to large scale coordinated DDoS and cracking attacks

• Internet can be vector for sophisticated attacks
  – Stuxnet probably developed by intelligence agencies
  – clean-up of agent.btz worm took 14 months

• Proxy servers can be used to attack and defense
  – to hide attack signature
  – to overpass filtering
Disruption Tolerance

Overview of Challenges

• Mobility
  - handoff, roaming failures
  - topology, routing, location management

• Connectivity
  - jamming
  - lossy wireless links

• Delay
  - interplanetary communication
  - disconnected operations

• Energy
  - resource constrained networks
  - e.g. WSN (wireless sensor networks)
Delay- and Disruption- Tolerance
Definitions

- **Delay tolerance**
  - network provides service to user even under long delay

- **Disruption tolerance**
  - network provides service to user even when disrupted
    - stable end-to-end path doesn’t exist

- **Challenged networks**
  - networks subject to environmental challenges
    - weak, episodic, and asymmetric connectivity from wireless links
    - mobility-induced dynamic behavior
    - unpredictably long delay
Communication Environment

Impact of Wireless Channel

- Open channel subject to *attack*
  - eavesdropping
    - network and traffic analysis
  - interference
    - jamming and denial of service
  - injection of bogus signalling and control messages
- Weak, intermittent, and episodic connectivity
Communication Environment

Impact of Wireless Channel

- Open channel subject to attack
- Weak, intermittent, and episodic connectivity
  - limited bandwidth of shared medium
  - time-varying available bandwidth
    - noise, weather (latter for free-space laser as well as RF)
  - episodic connectivity
    - channel fades between bit errors & failed links in consequence
    - difficult to achieve routing convergence
Communication Environment

Impact of Mobility

- Dynamic nodes and topologies
  - changing links, clustering, and federation topology
  - difficult to achieve routing convergence
- Control loop delay
  - mobility may exceed ability of control loops to react
- QoS
Communication Environment

Impact of Mobility

- Dynamic nodes and topologies
  - changing links, clustering, and federation topology
  - difficult to achieve routing convergence
- Control loop delay
  - mobility may exceed ability of control loops to react
- Impacts QoS
  - changes in inter-node distance
    - requires power adaptation
    - changes density and impacts degree of connectivity
  - latency issues (routing optimizations temporary)
Communication Environment
Impact of Mobility

• Dynamic nodes and topologies
  - changing links, clustering, and federation topology
  - difficult to achieve routing convergence

• Control loop delay
  - mobility may exceed ability of control loops to react

• Impacts QoS
  - changes in inter-node distance
    • requires power adaptation
    • changes density and impacts degree of connectivity
  - latency issues (routing optimizations temporary)
Communication Environment

Impact of Unpredictably High Latency

• Long inter-application delay appears to be disruption
  - long path \((c)\)
  - store-and-forward queueing due to episodic connectivity
  - latency masking techniques mitigate: caching, prefetching
    • but *don’t always* help
Communication Environment
Impact of Unpredictably High Latency

- Long inter-application delay appears to be disruption
- Severely impacts transport and network protocols
  - signalling latencies dominate at high data rates
  - very long control loops
    - long delays may cause data transfer to stall (window-based)
    - wrapped sequence number spaces
  - high-bandwidth-$\times$-delay products
    - real-time reaction to many bits in flight difficult or impossible
    - massive buffering required for error control
Resilience and Survivability
Assumptions and Challenges

- Problem cannot be solved at physical and link layers
  - assume that best physical, MAC, link techniques in use
  - diminishing returns on further research
- Strong connectivity will not always be achievable
  - economics and policy preclude connectivity everywhere
    - faraday cages for security
    - caves
    - nomadic hunters in northern Sweden; search and rescue in UK
- Network / security infrastructure may be unavailable
  - node failure or overrun (capture)
  - radio silence or jammed channel (enemy, cracker, DDoS)
  - compromised node software
Resilience and Survivability
Assumptions and Challenges

• Very long delay inevitable in some scenarios
  – path (speed of light) latency
    • satellite links
    • interplanetary (and intergalactic?) Internet
  – object transmission delay
    • large objects over modest data rates
    • weakly connected and congested links
  – store-and-forward over episodically connected paths

• Security and survivability are not binary choices
  – level of security must be traded against resource cost …
    • limited node power
    • limited channel bandwidth
… based on application requirements and user desires
Internet

Lessons and Risks

• Internet relatively resilient *as a whole* but...
  - significant risks exist
  - infrastructure insecure

• Internet best effort infrastructure subject to
  - congestion and flash crowds
  - DDoS attacks
Internet Lessons and Risks

- Internet infrastructure protocols not secure
  - BGP and DNS fragile and insecure
    - S-BGP and DNSsec deployment unlikely
  - disruptions not uncommon, e.g.:
    - 2005: Level3 cancels Cogent peering agreement
    - 2005: Comcast DNS meltdown
  - large scale disruptions possible
Internet Lessons and Risks

- Wireless access links significant vulnerability
  - insecurity of 802.11 WEP
  - DOS jamming potential of 802.11 and 802.16

- System insecurity provide vector, allow rapid spread
  - insecure Windows boxes with clueless users
  - vulnerable routers (Cisco IOS vulnerabilities)
  - vulnerable Web servers
  - no diversity to limit platform-specific threats, insider attacks
    - Intel x86
    - Microsoft Windows, IE, Outlook, Servers
    - Cisco IOS
Analysis of Systems
Computer and Communication Systems

• Tandem systems
  - hardware is improving
  - software base growing, leading to complex system
  - outage severity:
    • duration $\times$ number of processors $\times$ processor speed

• PSTN (public switched telephony network)
  - overload condition and human impacts the most
  - customer minutes to evaluate effect of a failure:
    • duration $\times$ number of customers

• HPC (high performance computing)
  - memory problems contribute most of the HW problems
Analysis of Systems

Internet Components

• Service failures
  – operator and software errors

• Regional networks
  – few links responsible for more than half of link failures

• BGP stability
  – short-lived outages, average failure rate in 25 days

• Backbone failures
  – 20% planned, 80% unplanned outage

• Datacenter failures
  – high number of restarts in early phases of server lifecycle
Challenges and Tolerance
Challenge Model and Taxonomy

• Motivation
• Past failures
• Challenge model and taxonomy
• Challenge tolerance
Network Challenge Taxonomy

Motivation

• Networks face challenges that are catastrophic
  – financial cost (e.g. billions of $ in case of worms)
  – potential for human loss (e.g. lack of 9-1-1 services)

• Understanding the network behavior is crucial
  – Future Internet architectures and design of new protocols
  – network engineering of existing networks

• Model challenges
  – for correct threat modelling for resilient network design

• Develop a taxonomy of challenges
  – establishing common terminology among researchers
Challenges to Normal Operation
Definition and Examples

• Challenge definition:
  - characteristic or condition that may manifest as an adverse event or condition that impacts the normal operation

• Broad challenge categories
  - large-scale disasters
  - socio-political and economic challenges
  - dependent failures
  - human errors
  - malicious attacks
  - unusual but legitimate traffic
  - environmental challenges
Definitions

Challenge → Fault → Error → Failure

- **Challenge**
  - adverse event or condition that impacts normal operation
  - external event that triggers a fault

- **Fault**
  - property of a system based on its design

- **Error**
  - stochastic event in either space (system) or time
  - manifestation of a *fault*

- **Service failure**
  - deviation of delivered service from service specification

[SHÇ+2010, ALR+2004]
ResiliNets Strategy

$D^2R^2 + DR$

- **Real time control loop:** $D^2R^2$
  - **defend**
    - passive
    - active
  - **detect**
  - **remediate**
  - **recover**

- **Background loop:** DR
  - **diagnose**
  - **refine**
Challenges and ResiliNets Strategy

Challenges:
- Disasters: natural, man-made
- Socio-political and economical factors
- Dependent failures
- Human errors
- Malicious attacks: DDoS
- Unusual traffic: flash crowds
- Environmental: mobility, connectivity, delay

Errors passed on to operational state

[SHÇ+2010, ÇS2013]
## Challenge Characteristics
### Spatial and Temporal Properties

<table>
<thead>
<tr>
<th>Challenge Examples</th>
<th>Spatial Region</th>
<th>Temporal Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>challenge</td>
<td>impact</td>
</tr>
<tr>
<td>earthquake</td>
<td>100s km²</td>
<td>100s km²</td>
</tr>
<tr>
<td>fire</td>
<td>100s m²</td>
<td>10s km²</td>
</tr>
<tr>
<td>hurricane</td>
<td>100s km²</td>
<td>100s km²</td>
</tr>
<tr>
<td>solar storm</td>
<td>1000s km²</td>
<td>1000s km²</td>
</tr>
<tr>
<td>misconfiguration</td>
<td>node</td>
<td>global</td>
</tr>
<tr>
<td>malicious attack</td>
<td>node</td>
<td>global</td>
</tr>
<tr>
<td>terrorism</td>
<td>100s km²</td>
<td>global</td>
</tr>
<tr>
<td>policy related</td>
<td>N/A</td>
<td>regional +</td>
</tr>
<tr>
<td>deepering</td>
<td>N/A</td>
<td>global</td>
</tr>
<tr>
<td>pandemic</td>
<td>global</td>
<td>global</td>
</tr>
<tr>
<td>power blackout</td>
<td>100s km²</td>
<td>regional</td>
</tr>
</tbody>
</table>
Challenge Taxonomy
Overview

- Classification and taxonomy of challenges
  - based on fault taxonomy
    - [ALR+2004] and IFIP 10.4 related publications

- Elementary challenge classes
  - elementary orthogonal classification within fault groups
Challenge Taxonomy
Elementary Challenge Classes

• Elementary challenge classes
  - phenomenological cause
  - system boundary
  - target
  - objective
  - intent
  - capability
  - dimension
  - domain
  - scope
  - significance
  - persistence
  - repetition

• Based on 10.4 fault taxonomy
  - some correspond directly; some new
  - not all binary choices, some multiple levels
  - not all combinations possible
    • e.g. natural challenges (phenom.) can’t be malicious (objective)
Challenge Taxonomy
Phenomenological Cause: Human vs. Natural

Phenomenological cause

- **Natural challenges**
- terrestrial e.g. earthquakes
- meteorological e.g. hurricanes and ice storms
- cosmological e.g. CMEs (coronal mass ejections)

- **Human challenges**
- social e.g. recreational cracker
- political and ethnic e.g. political unrest
- business and economic e.g. depeering
- terrorism e.g. 9/11 and London bombings

- **Dependencies**
Challenge Taxonomy
Phenomenological Cause: Dependencies

Phenomenological cause

- **Natural challenges**
- **Human challenges**
- **Dependency**
  - *lower level failure* challenging higher layers of infrastructure
    - e.g. cable cuts, Georgian woman cutting Armenian Internet
  - *cascading failure* propagating at a given level
    - e.g. incorrect BGP prefix propagation
  - *interdependent infrastructure* impact separate infrastructure
    - e.g. power grid failure on net
System boundary

- **Internal challenge**
  - challenge within a system of interest
  - e.g. challenge within an autonomous system

- **External challenge**
  - challenge impact by external environmental factors
  - can be considered system of systems
  - e.g. impact of power grid on Internet
Challenge Taxonomy

Target

- **Direct challenge**
  - challenge directed at the infrastructure that may fail
  - e.g. sabotage on cables

- **Collateral damage**
  - challenge directed at interdependent infrastructure
  - e.g. 9/11 was not targeted at Internet or PSTN
Objective

- **Malicious**
  - introduced by human with intent to harm system
  - may be automated (e.g. Botnet)

- **Selfish**
  - introduced with selfish intent (e.g. not cooperating)

- **Non-malicious**
  - introduced without malicious objective
  - include all *natural challenges*
  - include *human deliberate incompetence challenges*
  - include *human non-deliberate accidental challenges*
Challenge Taxonomy

Intent

- **Deliberate challenge**
  - result of a harmful decision

- **Non-deliberate challenge**
  - introduced without awareness
  - include mistakes
Challenge Taxonomy

Capability

- **Accidental challenges**
  - introduced inadvertently

- **Incompetence challenges**
  - from lack of professional competence by authorised humans
  - inadequacy of development or deployment organisation
Challenge Taxonomy

Dimension

• **Hardware challenge**
  - target hardware: network components and physical links

• **Software challenge**
  - target software: operating systems and protocol software

• **Protocol challenge**
  - target protocol operation and signalling

• **Traffic challenge**
  - impact traffic such as flash crowd and DDoS
Challenge Taxonomy
Domain: Medium & Mobility

Domain

- **Medium**
  - wired: target wired network infrastructure
  - wireless: wireless medium and related components
  - hybrid ???

- **Mobility**
  - fixed: nodes are located at fixed locations
  - mobile: nodes are mobile, requires topology control

- **Delay**
- **Energy**
Challenge Taxonomy
Domain:  Delay & Energy

Domain

• **Medium**

• **Mobility**

• **Delay**
  - low delay:  e.g. terrestrial networks
  - predictable high delay:  e.g. interplanetary communication
  - unpredictable high delay:  e.g. sensor for habitat monitoring

• **Energy**
  - grid:  e.g. desktop connected to power grid
  - replaceable battery:  e.g. laptop with limited energy
  - energy constrained:  e.g. sensor node in hostile environment
Scope

- **Node challenges**
  - target nodes: switches, routers, and other components

- **Link challenges**
  - target wired links or wireless spectrum

- **Area challenges** affect nodes and links
  - *local* challenge with a local scope
  - *regional* challenge with a regional scope
    - *fixed* challenge over a given area
    - *evolving* challenge moving or changing in area
  - *global* challenge with a global scope
Challenge Taxonomy

Significance

related to ATIS T1A1 extent in (U,D,E) triple

- **Minor challenges**
  - small in scope or intended consequences

- **Major challenges**
  - large in scope or intended consequences
  - include large areas and attacks against critical subsystems

- **Catastrophic challenges**
  - catastrophic in scope or intended consequences
  - include very large areas
  - include attacks against many critical subsystems
Persistence

- **Persistent challenges** from an adverse condition
  - *short-lived challenges*
  - *long-lived challenges*
  - remediation important during challenge
  - recovery after adverse condition ends

- **Transient challenges** from adverse events
  - single event challenges
  - remediation needed if physical infrastructure destroyed
  - recovery most important after challenge event
Challenge Taxonomy

Repetition

- **Single challenge**
  - single instance of a given challenge
- **Multiple challenge**
  - repeated instance of a given challenge
- **Adaptive challenge**
  - repeated instance of a challenge that adapts to failures
Challenges and Tolerance

Challenge Tolerance

- Motivation
- Past failures
- Challenge model and taxonomy
- Challenge tolerance
ResiliNets Principles

Enablers

- P9: self-protection – defend from challenges
- P10: connectivity – connectivity and association maintained
- P11: redundancy – multiple components or mechanisms
- P12: diversity – provide alternatives
- P13: multilevel resilience – between protocols, planes
- P14: context awareness – necessary to detect challenges
- P15: translucency – control abstraction between levels
Resilient Networks
Sub-Disciplines: Challenge Tolerance

- **Survivability**: many ∨ targeted failures
- **Fault Tolerance**: few ∧ random
- **Traffic Tolerance**: legitimate flash crowd attack DDoS
- **Disruption Tolerance**: environmental delay mobility connectivity energy

- Trustworthiness
  - Dependability: reliability maintainability safety
  - Security: availability integrity confidentiality nonrepudiaiblity AAA
  - Performability: auditability authorisability authenticity
  - QoS: measures

- Fault Tolerance
- Disruption Tolerance
- Traffic Tolerance
- Survivability

4 February 2016

MST CPE 6510 – Challenges and Tolerance
Fault Tolerance
Type of Discipline

• Fault-tolerance is related to challenges
  – subset of survivability
  – peer to disruption-tolerance and traffic-tolerance

• FT measured by trustworthiness disciplines
  – dependability: availability, reliability, etc.
  – performability
  – security
Fault Tolerance

Definition

• **Fault tolerance**
  - avoid service *failures* in the presence of *faults*

• Mature discipline
  - generally assumes *independent random* faults
  - traditional fault models do *not* hold under
    • malicious attack and large-scale disaster
    • generally the domain of *survivability*
Fault Tolerance
Confusion with Survivability

• Some communities use survivability to mean FT
  – optical networking community: “survivable optical rings”
Fault Tolerance Techniques
Redundancy and Diversity

• Redundancy is the fundamental FT technique
  - **redundancy**: multiple components or mechanisms
  - **diversity**: alternatives in components or mechanisms
  - primarily a survivability technique
Redundancy Techniques

• Redundancy: replication of parts or modules of system
  • components, e.g. electronic circuits, switches, links
  • information, e.g. packets, communication circuits
  • algorithms, e.g. N-version programming
  – permit operation even when some parts have failed
Redundancy

$M$-of-$N$ Redundancy

- $M$-of-$N$ redundancy
  - $N$ modules in system
  - $M$ modules needed to maintain operational state
  - $(N - M) + 1$ module failures
    - cause error
    - that may result in system failure (at the next higher level)
Redundancy

\( M \)-of-\( N \) Important Cases

- **1+1 redundancy**
  - **1:1 redundancy**
    - every component has a backup
    - duplex or dual modular redundancy (DMR)
    - 1-of-2 in \( M \)-of-\( N \) terminology

- **N+1 redundancy**
  - **1:N redundancy**
    - one redundant component for a group of \( N \)
    - \( N \)-of-(\( N+1 \)) in \( M \)-of-\( N \) terminology
Redundancy

$M$-of-$N$ Alternative Use of Redundancy

- **Hot standby**
  - unused; ready for substitution

- **Dynamic redundancy**
  - used but ready to load balance
    - useful for processors and networking
    - may result in service degradation

- **Choice based on**
  - probability of error
  - degradation-tolerance of service
Critical Infrastructure
Need for Survivability

• Critical infrastructures need to be *survivable*
  – continue to operate when challenged
• Fault-tolerance insufficient for correlated failures
  – area-based challenges
    • large-scale natural disasters, e.g. Katrina
    • accidents, e.g. NE US power failure
  – targeted challenges
    • attacks against physical or software infrastructure
Survivability Definitions

• **Survivability**
  - capability of a system to fulfill mission in a timely manner
  - in presence of *large-scale disasters, attacks*, failures

• Characteristics [EFL+1999]
  - mission: set of high-level requirements or goals
    - reasonable/expected behaviour during impairments
  - lacks multilevel view
  - often measured with dependability & performance metrics
  - applied to unbounded systems
    - distributed control, limited visibility and unpredictable growth
  - *mission fulfilment* must survive, even when system does not
Survivability
Challenges Addressed

• *Subset of challenges addressed*
  
  - large-scale disasters
    - natural (e.g. hurricane, tsunami, coronal mass ejection)
    - human-caused (e.g. power failure, EMP weapon)
  
  - socio-political and economic challenges
  
  - dependent failures
  
  - unintentional misconfiguration or operational mistakes
  
  - malicious attacks
  
  - environmental challenges
    - mobility, weak connectivity, unpredictable delay
  
  - unusual but legitimate traffic (e.g. flash crowd)
Survivability

Relationship to Other Disciplines

- Survivability is subset of challenge tolerance
  - subset of resilience
  - peer to disruption-tolerance and traffic-tolerance
  - distinguished from fault tolerance by:
    - scope: large scale correlated failures
    - criticality: failures due to targeted attack
- Survivability measured by trustworthiness disciplines
  - dependability: availability, reliability, etc.
  - performability: level or performance
  - security
Survivability
Relationship to Other Disciplines

- Survivability
  - highly correlated failures
    - spatial (e.g. disaster)
    - temporal (e.g. attack)
  - objective
    - malicious attacks
    - non-malicious events

- Fault tolerance
  - random failures
    - component level
    - single or at most few
  - objective
    - generally non-malicious
Survivability
Relationship to Other Disciplines

- Survivability
  - survivability is robustness under attack
  - considers a range of survivability levels
  - emphasizes performance of a compromised system

- Security
  - security is hardness to attacks
  - security is traditionally considered binary
    - but really spectrum
  - does not consider performance of a compromised system
Survivability Techniques
Redundancy for Fault Tolerance

- Redundancy: multiple components or mechanisms
  - fundamental and primary technique for fault-tolerance
  - recall: fault tolerance is a subset of survivability
Diversity
Definition and Measure

• Diversity consists of providing alternatives
  - when challenges impact particular alternatives other alternatives prevent degradation
  - degree of diversity: number of different alternatives
  - alternative can either be:
    • simultaneously operational to defend
    • available for use as needed to remediate
Diversity

Spatial

- **Diversity**: consists of providing different alternatives
- **Spatial diversity**: diversity across space
  - requires degree of at least redundancy degree
  - **topological diversity**: across logical network topology
  - **geographic diversity**: across physical network topology
  - both are necessary **why?**

- Temporal diversity
- Operational diversity
Diversity

Spatial

• \textit{Diversity} consists of providing different alternatives

• \textit{Spatial diversity}: diversity across space
  – requires degree of at least redundancy degree
  – \textit{topological diversity}: across logical network topology
  – \textit{geographic diversity}: across physical network topology
  – both are necessary: logical and physical topology entwined

• Temporal diversity

• Operational diversity
Diversity

Temporal

• *Diversity* consists of providing different alternatives
• *Spatial diversity*: diversity across space
• *Temporal diversity*: diversity in time
  - e.g. variation to resist traffic analysis
• Operational diversity
Diversity
Operational

- **Diversity** consists of providing different alternatives
- **Spatial diversity**: diversity across space
- **Temporal diversity**: diversity in time
- **Operational diversity**: implementation & mechanism examples?
Diversity

Operational

• **Diversity** consists of providing different alternatives

• **Spatial diversity**: diversity across space

• **Temporal diversity**: diversity in time

• **Operational diversity**: implementation & mechanism
  - implementation: e.g. protocol or OS choices
    • monoculture avoidance (MS-Windows, IOS, TCP/IP)
  - medium: e.g. wired and wireless
  - mechanism: e.g. open vs. closed loop (ARQ vs. FEC)
Diversity Examples

- Example
  - mechanism diversity: wired vs. wireless
    - compensate for interference vs. fiber cut
  - provider diversity: multi-homed
  - spatial diversity: geographic diversity in paths
Resilience
Multilevel

• Multilevel resilience
  7  application
  4  end-to-end transport
  3r path routing
  3t topology
  2  physical links and nodes

• Resilience techniques to be applied at each level
  – each level provides a foundation for resilience above
  – each level provides a service
    • whose properties dictate the resilience of that service
    • and guide the mechanisms and design above
Multilevel Resilience
2: Physical Network Infrastructure

- Physical network infrastructure
  - nodes
  - links
- Service provided
  - links and nodes that from which a topology can be formed
- Redundancy and diversity applied
Multilevel Resilience

3t: Topology Survivability

- Topology survivability
  - diversity (and redundancy) in topology
- Diversity in topology
  - graph properties must include geography
    - distance-based diversity metric determined by threat model
Multilevel Resilience
3r: Path Routing Survivability

• Path routing survivability
  – diversity (and redundancy) in path routing

• Multipath routing with diversity
Multilevel Resilience
4: End-to-End Transport Survivability

- End-to-end survivability
  - diversity (and redundancy) in end-to-end transport
- Multipath transport with diversity
  - explicit support for multipath transport
  - spreading across paths (e.g. erasure coding)
Multilevel Resilience
7: Application Survivability

• Application survivability
  – diversity (and redundancy) in networked applications
References and Further Reading


References and Further Reading


• Some slides are adopted from “KU EECS 983 – Resilient and Survivable Networking” class taught by Prof. James P.G. Sterbenz

End of Foils