Resilient Networks
Missouri S&T University CPE 6510
Resilience Overview

Egemen K. Çetinkaya
Department of Electrical & Computer Engineering
Missouri University of Science and Technology

cetinkayae@mst.edu

http://web.mst.edu/~cetinkayae/teaching/CPE6510Spring2016
Resilience Overview

Outline

• Motivation
• Past failures (introduction)
• Resilience disciplines
• Architectural framework
Resilience Overview

Motivation

• Motivation
• Past failures (introduction)
• Resilience disciplines
• Architectural framework
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
Resilience Overview
Past Failures (Introduction)

• Motivation
• Past failures (introduction)
• Resilience disciplines
• Architectural framework
Past Failures and Disasters Overview

- Brief chronological overview of *selected* past failures
  - introduction to a wide variety of challenges
  - introduction to the lessons learned
    - current threats and vulnerabilities
    - changes needed to improve resilience of Future Internet
  - significantly more detail later
    - next week and [ÇS2013]
    - 1st round of student presentations
Past Failures and Disasters

Selected Chronology

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
Past Failures and Disasters

Hinsdale Central Office Fire

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
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
### Past Failures and Disasters

**Baltimore Tunnel Fire**

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1988</td>
<td>Hinsdale Illinois Bell central office fire</td>
</tr>
<tr>
<td>2001</td>
<td>Baltimore tunnel fire</td>
</tr>
<tr>
<td>2001</td>
<td>9/11 terrorist attacks</td>
</tr>
<tr>
<td>2003</td>
<td>Cogent peering disputes</td>
</tr>
<tr>
<td>2003</td>
<td>Northeast US blackout</td>
</tr>
<tr>
<td>2005</td>
<td>7/7 terrorist attacks</td>
</tr>
<tr>
<td>2005</td>
<td>Hurricane Katrina</td>
</tr>
<tr>
<td>2006</td>
<td>Hengchun earthquake</td>
</tr>
<tr>
<td>2007</td>
<td>International information warfare</td>
</tr>
<tr>
<td>2008</td>
<td>Pakistan YouTube hijack</td>
</tr>
<tr>
<td>2008</td>
<td>Mideast submarine cable cuts</td>
</tr>
<tr>
<td>2010</td>
<td>Arab Spring</td>
</tr>
<tr>
<td>20??</td>
<td>H1N1 Influenza pandemic</td>
</tr>
</tbody>
</table>
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
Past Failures and Disasters

9/11 Terrorist Attacks

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
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
Past Failures and Disasters

Peering Disputes

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
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 involved in many peering disputes
    • e.g. AOL, France Telecom, Level 3, TeliaSonera, Sprint-Nextel
Peering Disputes

Lessons

• Network ops of depends on \textit{nontechnical} factors
  - policy
  - economics
  - regulation
• Can result in significant network disruptions
Past Failures and Disasters
Northeast US Blackout

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
NE Power Failure Overview

• 265 power plants with 508 generating units offline
• ~10M without power
  – OH, MI, PA, NY, QC
• Many 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
  – no significant role of Blaster and other worms
• CERT, RCMP, NCS joint study

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
Past Failures and Disasters

7/7 Terrorist Attacks

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
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
Past Failures and Disasters

Hurricane Katrina

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
Hurricane Katrina Overview

• 2005: Hurricane Katrina
  - evolves from TD 12 on 23 Aug. to cat. 5 landfall 29 Aug.
  - significant wind damage on coast spares New Orleans
  - then storm surge puts 60–80% of NO under water

• Many correlated infrastructure failures
  - power grid: 2.6M out, some for a month
  - PSTN out, most cell towers out
  - network facilities down
    • loss of power and flooding
  - incompatible communications
    • in spite of 9/11 lessons
Hurricane Katrina Lessons

• Threat was well known
  – including Oct. 2004 *National Geographic* article

• 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 equipment staging response insufficient
Past Failures and Disasters

Hengchun Earthquake

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
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
Past Failures and Disasters

International Information Warfare

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
International Information Warfare Overview

• Information warfare among political groups
• 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
  – e.g. against RIAA and MPAA after MegaUpload seizure
International Information Warfare

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
Past Failures and Disasters
Pakistan YouTube Hijack

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
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
Past Failures and Disasters

Mideast Submarine Cable Cuts

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  H1N1 Influenza pandemic
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 ASs down

• Cause undetermined
  - accidental cuts frequent (dragging anchors, friction against rock)
Mideast Submarine Cable Cuts

Lessons

• Mideast has limited cable service
  – geographically concentrated

• Redundancy without diversity is not resilient
Past Failures and Disasters

Arab Spring

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  Influenza pandemic
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
Past Failures and Disasters

Influenza Pandemic

1988  Hinsdale Illinois Bell central office fire
2001  Baltimore tunnel fire
2001  9/11 terrorist attacks
2003  Cogent peering disputes
2003  Northeast US blackout
2005  7/7 terrorist attacks
2005  Hurricane Katrina
2006  Hengchun earthquake
2007  International information warfare
2008  Pakistan YouTube hijack
2008  Mideast submarine cable cuts
2010  Arab Spring
20??  Influenza pandemic
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 did not become a long-lived serious pandemic
H1N1 Influenza Pandemic Risks

• H1N1 did not have major impact
  – but the influenza pandemic potential is severe and likely
• Many organisations still 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
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 deployment unlikely
    - DNSSEC is more promising for deployment
  - disruptions not uncommon, e.g.:
    - 2005: Level 3 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
Resilience Overview

Resilience Disciplines

• Motivation
• Past failures (introduction)
• Resilience disciplines
• Architectural framework
Challenge Definition

Challenges and Threats

• **Challenge**
  - adverse event or condition that impacts normal operation
    • large-scale disasters
    • socio-political and economic challenges
    • dependent failures
    • human errors caused by accidents or incompetence
    • malicious attacks from intelligent adversaries
    • unusual but legitimate traffic load such as a flash crowd
    • environmental challenges in wireless medium
  - event that triggers a fault

• **Threat**
  - potential *challenge* that might exploit a *vulnerability*
Challenge → Fault → Error → Failure

Faults and Vulnerabilities

• **Challenge** →

• **Fault**
  - property of a system based on its design
  - cause of an **error**
    • *dormant* (or latent) when it does not yet cause an error
    • *active* when it causes an error
  - may be internal or external to a given system
  - cannot be directly observed
    • no such thing as “fault detection”

• **Vulnerability**
  - internal fault that allows an external fault to cause an error

[ALR+2004]
Challenge → Fault → Error → Failure

**Errors**

- **Challenge → Fault →**
- **Error**
  - stochastic event in either space (system) or time
  - manifestation of a *fault*
  - system state that may lead to a subsequent failure
  - errors can be detected
    - and used for *fault diagnosis*

[ALR+2004]
Challenge → Fault → Error → Failure

Failures

- **Challenge → Fault → Error →**
- **Service failure**
  - deviation of delivered service from service specification
  - may result from an error (but may not)
  - transition from correct to incorrect service state
    - *service outage*: incorrect service state
    - *timing failure*: performance degradation
    - *content failure*: incorrect information
- **Service restoration**
  - transition from incorrect to correct service state

[ALR+2004]
Resilience Disciplines Overview

- Challenge Tolerance
- Trustworthiness: measurable quantities
- Robustness:
  - control theoretic notion
  - $\Delta$ trustworthiness under challenge
Resilient Networks
Sub-Disciplines: Challenge Tolerance

- Fault tolerance
  - tolerate one (or several) random failures

- Survivability against attack and large-scale disasters
  - tolerate many and correlated failures

- Disruption tolerance
  - mobility, weak/episodic connectivity, unpredictably long delay
  - energy and power constraints

- Traffic tolerance
  - DDoS attacks
  - legitimate traffic such as flash crowds
    sufficiently sophisticated DDoS attack indistinguishable from legitimate traffic
Resilient Networks

Sub-Disciplines: Challenge Tolerance

- **Survivability**: many $\lor$ targetted failures
- **Fault Tolerance**: few $\land$ random failures
- **Traffic Tolerance**: legitimate, flash crowd, attack, DDoS
- **Disruption Tolerance**: environmental delay, mobility, connectivity, energy

**Trustworthiness**
- **Dependability**: reliability, maintainability, safety
- **Availability**: availability, integrity
- **Confidentiality**: confidentiality
- **Security**: AAA, nonrepudiability, auditability, authorisability, authenticity
- **Performability**: QoS measures, maintainability, safety
Resilient Networks
Sub-Disciplines: Trustworthiness

• Dependability
  - availability: probability ready for service (MTTF/MTBF)
  - reliability: probability of continuous service for time interval
  - safety: probability of no catastrophic consequences
  - maintainability, integrity

• Security
  - AAA: auditability, authorisability, authenticity
  - confidentiality, integrity, availability, nonrepudiability

• Performability
  - traditional performance metrics
Resilient Networks
Sub-Disciplines: Trustworthiness
Resilient Networks
Robustness and Complexity

• Resilience
  – challenge tolerance + trustworthiness + robustness

• Robustness
  – insensitivity of trustworthiness parameters to challenges
  – fragility = 1/robustness

• Complexity
  – measure of computational aspects of intricacy of a system
  – memory (state)
  – processing (state machines)
  – interconnection (topology)
Scope of Resilience
Relationship to Other 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

- **Robustness Complexity**

- **Trustworthiness**
  - Dependability
    - reliability maintainability safety
  - availability integrity
  - Security
    - confidentiality nonrepudiability
    - auditability authorisability
    - authenticity
  - Performability
    - QoS measures

- **Fault Tolerance**
  - (few ∧ random)
  - many ∨ targetted failures

- **Disruption Tolerance**
  - environmental delay mobility connectivity energy

- **Traffic Tolerance**
  - legitimate flash crowd
  - attack DDoS

- **Performability**
  - QoS measures

- **Challenge Tolerance**
  - Survivability
    - many ∨ targeted failures
  - Fault Tolerance (few ∧ 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 ∧ random)
  - many ∨ targetted failures

- **Disruption Tolerance**
  - environmental delay mobility connectivity energy

- **Traffic Tolerance**
  - legitimate flash crowd
  - attack DDoS

- **Performability**
  - QoS measures
Dependability
Definition

• **Dependability**
  - reliance can be placed on delivered service

• Dependability aspects
  - availability: readiness for usage
  - reliability: continuity of service
  - safety: non-occurrence of catastrophic consequences
  - integrity: non-occurrence of improper information alterations
  - maintainability: aptitude to undergo repairs and evolution
Reliability and Availability

Reliability Definition

- **Reliability**
  - probability of a system performing its purpose adequately
  - for the period of time intended
  - under the operating conditions intended
Reliability and Availability

Availability Definition

- **Availability**
  - probability of a system operational at a given time
  - initially follows reliability curve
    - but then repairs keep availability higher
  - steady state: uptime / observation time
Security Definitions

- **Security**
  - confidentiality: non-occurrence of unauthorized disclosure
  - integrity: message hasn’t been altered
  - availability: information is available when needed
  - nonrepudiation (sender can’t deny sending)
  - AAA: authentication, authorization, accounting
Resilience Disciplines
Degradable Systems

- *Degradable systems*
  - relationship between performance and reliability
  - degraded performance during challenges
    - without complete failure
  - performance as a second dimension of reliability
    [Huslende-1981]
Resilience Disciplines

**Performability Definition**

- **Performability**
  - capability to deliver performance required by a service
    - as specified in the service spec
    - described by QoS measures
    - when challenged
  - probability that the system
    - will stay above a certain accomplishment level
    - over a fixed period of time
  [M1980, M1992]
Resilience Disciplines
Relationship of Performability

- **Performability**
  - subset of trustworthiness
  - measures performance of system when challenged

- Tight relationship with **dependability**
  - availability and reliability binary: system up or down
  - performability gives performance level given up
  - degradable performance
Resilience Disciplines
Performability Formal Definition

- **Performability**: \( \text{perf} (B) = \Pr[Y \in B] \)
  - probability that \( S \) performs at a level in \( B \)
  - over a specified period of time \( T \)

\( B \subseteq A \): measurable set of accomplishment levels \( B \)
  - among all possible performance outcomes \( A \)

\( Y \): random variable representing a performance metric

\( S = C \cap E \): system in its environment
  - \( C \): object system
  - \( E \): environment (workload, traffic, challenges)
Survivability

Definitions

- **Survivability**
  - capability of a system to fulfill mission in a timely manner
  - in presence of large-scale natural disasters, attacks, failures
Resilience Disciplines
Disruption Tolerance Definition and Scope

• *Disruption tolerance* is the ability of a system to tolerate disruptions in connectivity among its components

• Disruption tolerance includes tolerance of
  – environmental challenges
    • weak and episodic channel connectivity
    • mobility
    • delay tolerance
  – energy and power constraints
Resilience Disciplines
Traffic Tolerance Definition

- **Traffic tolerance**
  - ability to avoid service *failures*
    - significant drop in carried load including congestion collapse
  - in the presence of traffic
    - beyond design specification of network
    - expected for normal operation
Resilience Disciplines
TT Challenges: Legitimate Flash Crowd

- **Flash crowd**
  - legitimate traffic beyond expected for normal operation
- Occurs in response to a triggering event
  - disaster or significant news event
    - can overwhelm new Web sites
    - can overwhelm mobile telephone networks
  - publicity for an obscure Web site called *slash-dotting*
    - article on slashdot.org frequently brings down Web servers
Resilience Disciplines

TT Challenges: Malicious DoS

- **DoS**: denial of service attack
  - injection of information or traffic
    - traffic competing with legitimate users
    - signalling messages that prevent normal access
    - jamming of RF signals
  - intended to deny access to a resource
    - reduce availability or cause total failure of a system
  - can frequently be traced to source
    - throttled or shut down
Resilience Disciplines

TT Challenges: Malicious DDoS

- **DDoS**: distributed denial of service attack
  - distributed DoS
    - intended to deny access to a resource as with DoS
  - injection of traffic from *many* sources
    - far more difficult to shut down than single-source DoS
    - sufficiently sophisticated DDoS attack indistinguishable from legitimate traffic
Robustness
Definitions

- Robustness
  - control system operates in the face of uncertainty
  - remains stable under varying inputs
Resilience Definition

- **Resilience**
  - the capability of network to provide and maintain
  - acceptable level of service
  - in the face of various challenges to normal operation
Resilience
Service

• Resilient service to applications
  - ability to access information
    • e.g. Web browsing, sensor monitoring
  - maintenance of end-to-end associations
    • e.g. video- and teleconference
  - operation of distributed processing and networked storage
Resilience Overview

Architectural Framework

- Motivation
- Past failures (introduction)
- Resilience disciplines
- Architectural framework
ResiliNets Axioms

IUER: Inevitable

A0. Faults are inevitable

• Not possible to construct perfect system
  – internal faults will exist

• Not possible to prevent challenges and threats
  – external faults will occur
ResiliNets Axioms

IUER: Understand

A1. Understand normal operations

- **Normal operation**: no adverse conditions present
  - loosely corresponds to PSTN and Internet design
    - e.g. PSTN: traffic engineering for Mother’s Day, not 9/11

- Leads to understanding when network is:
  - challenged
  - threatened
A2. Expect inevitable adverse events and conditions

- **Adverse event/condition**: challenge normal operation

- **Anticipated**: predictable based on
  - past events
  - threat analysis

- **Unanticipated**: not predictable with specificity
  - still need to be prepared in general sense

- Motivates part of $D^2R^2 + DR$ strategy
  - defend
  - detect
ResiliNets Axioms

IUER: Respond

A3. Respond to adverse events and conditions

• Respond to adverse events by remediation
  – graceful service degradation if necessary
    • permit timing failure
  – ensure correct operation
    • prevent content failure

• Motivates part of $D^2R^2 + DR$ strategy
  – remediate (immediately)
  – recover
  – diagnose and refine (long term)
Resilient Networks
ResiliNets Architectural Model

- ResiliNets Cube
  - multilevel
    - protocol layers
    - planes
    - mechanisms
- $D^2R^2+DR$ strategy
  - defend
  - detect
  - remediate
  - recover
  - diagnose
  - refine

mechanisms

resilience strategy

D2R2+DR

physical

MAC

cross-layer composable programmable & autonomic redundant & diverse context-aware & adaptive

management plane

control plane

data plane

architecture & engineering

adaptive applications & overlays

application

session

E2E

ARQ

FEC

network

EC

APR

HBH link

ARQ

FEC

MAC

CDMA

UDMA

physical

MAC

HBH link

network

management plane

control plane

data plane

architecture & engineering

adaptive applications & overlays

application

session

E2E

ARQ

FEC

network

EC

APR

HBH link

ARQ

FEC

MAC

CDMA

UDMA

physical

MAC

HBH link

network
ResiliNets Strategy

$D^2R^2 + DR$

- **Real-time control loop:** $D^2R^2$
  - defend
    - passive
    - active
  - detect
  - remediate
  - recover
- **Background loop:** DR
  - diagnose
  - refine
ResiliNets Strategy

\[ D^2R^2 + DR: \text{ Defend (Passive)} \]

S1a. Defend against challenges to normal operation

- Reduce the probability of a fault leading to a failure
- Reduces the impact of an adverse event
- Analogy
  - thick outer and inner castle walls
- Examples
  - spatially diverse redundant paths
ResiliNets Strategy

Real-Time Control Loop $D^2R^2 + DR$

- Real-time control loop: $D^2R^2$
  - real-time with respect to network operation
  - many simultaneous independent loops
- Background loop: DR
S1b. Defend against challenges to normal operation

- Reduce the probability of a fault leading to a failure
- Reduces the impact of an adverse event
- Analogy
  - lookout guard on castle wall
- Examples
  - filtering traffic for known attack signatures
ResiliNets Strategy

$D^2R^2 + DR$: Detect

S2. Detect when an adverse event or condition occurs

• Determine when defenses
  – have failed and remediation needs to occur
  – need to be strengthened

• Analogy
  – detect hole in wall from trebuchet

• Example
  – detection of behavioral anomaly
    • traffic load or pattern
    • protocol control messages
ResiliNets Strategy

\( D^2 R^2 \) + DR: Remediate

S3. Remediate during adverse condition

- Do the best possible
  - after adverse event / during adverse condition

- Corrective action at all levels
  - graceful degradation
  - correct operation

- Analogy
  - send subjects to inner wall; pour boiling oil over hole

- Examples
  - reroute network traffic
ResiliNets Strategy

$D^2R^2 + DR$: Recover

S4. Recover to normal operations

- Return to original state once adverse condition over
  - redeploy infrastructure
  - restore normal control and management

- Analogy
  - repair hole in wall

- Example
  - restore original network routing
ResiliNets Strategy

Background Control Loop: \( D^2R^2 + DR \)

- Real-time control loop: \( D^2R^2 \)
- Background loop: \( DR \)
  - out-of-band analysis of the reaction to adverse events
  - increase resilience of system
ResiliNets Strategy

$D^2R^2 + DR$: Diagnose

S5. Diagnose fault that lead to error or failure

- Root cause analysis to discover design flaws
  - faults not directly detectable
- Analogy
  - analyze wall-thickness to trebuchet projectile weight ratio
- Example
  - analyze packet traces to determine protocol vulnerability
S6. Refine behavior for the future

- Learn from past $D^2R^2$ cycles
  - better defense, detection, remediation *next time*

- Analogy
  - build thicker castle wall
  - build watch tower for advance warning

- Example
  - enrich network topology
  - redesign protocols
Challenge → Fault → Error → Failure

Challenges and ResiliNets Strategy

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

Challenges

Detect

Defend

Errors passed on to operational state

[SHÇ+2010, ÇS2013]
ResiliNets Principles

High Level Grouping

- Prerequisites
- Tradeoffs: recognise and organise complexity
- Enablers
- Behaviour: require significant complexity to operate
ResiliNets Principles

Meta-Principles

• Small number of broad architectural principles
  – $O(10)$
    • enough to be useful
    • few enough to not overwhelm
  – e.g. redundancy, diversity, resource tradeoffs

• Refined and instantiated to specific contexts
  – layers, planes, network architecture
  – e.g. fault tolerant network components (redundancy)
  – e.g. spatially diverse redundant paths (redundancy+diversity)
    • but don’t replicate *everything*! (resource tradeoffs)
ResiliNets Principles

Prerequisites

- **P1**: service requirements
- **P2**: normal behaviour
- **P3**: threat and challenge models
- **P4**: metrics
- **P5**: heterogeneity
P1: Service requirements determine network resilience
   - applications and users determine level of resilience needed
   - information access and communication association
   - not all applications need service of high resilience
ResiliNets Principles

Normal Behaviour

P2: Normal behaviour to understand normal operations
- specification of system design with constraints in behaviour
- functional verification of design
- monitoring & learning normal behaviour of the system in situ
- refinement of behaviour specification and constraints
ResiliNets Principles

Threats

P3: Threat models to understand & detect challenges

- threat model needed to:
- understand, define, implement mechanisms that:
- defend, detect, and remediate
ResiliNets Principles
Metrics to Measure and Engineer

P4: Metrics needed to measure and engineer resilience

- metrics needed to determine effects of adverse event
- metrics determine satisfaction of P1
- challenge: how to derive resilience metric $0 \leq \mathcal{R} \leq 1$
  - from conventional performance metrics
  - topology, channel, traffic, mobility, …
P5: Heterogeneity

- trust and policy boundaries: tussle
- economic realities
- regulatory realities
- legacy networks (IP-based Internet, PSTN)
ResiliNets Principles

Tradeoffs

- P6: resource tradeoffs
- P7: complexity
- P8: state management
ResiliNets Principles

Resource Tradeoffs

P6: Resource tradeoffs
- resources are not infinite: traded against one-another
  - P: processing
  - B: bandwidth (rate)
  - L: latency constraint
  - M: memory
  - E: energy and power
  - £$: cost

• Type: choice
P7: Complexity

- significant complexity inherent and necessary
- resilience mechanisms increase complexity
  - which increases system vulnerability
- reduce unnecessary complexity and specification
ResiliNets Principles

State Management

P8: State management

- **stateless** vs. **soft state** vs. hard state
- **distributed** vs. mirrored vs. centralized
- **tolerance of inconsistent** vs. requirement for consistent
- resilience typically (but not always) suggests choices in bold

• Type: choice
ResiliNets Principles

Enablers

- P9: self-protection
- P10: connectivity
- P11: redundancy
- P12: diversity
- P13: multilevel resilience
- P14: context awareness
- P15: translucency
ResiliNets Principles

Self-Protection

P9: Self-protection essential to defend from challenges

- secure control mechanisms
  - AAA: authentication, authorisation, accounting
- information assurance mechanisms
  - confidentiality, integrity, nonrepudiation
- containment, firewalls, enclaves, …
P10: Connectivity and association maintained

- maintain connectivity when practical
- communicate even when strong connectivity not possible
  - disruption tolerant communication mechanisms
  - store-and-forward when necessary
  - store-and-haul (store-carry-forward)
ResiliNets Principles

Redundancy

P11: Redundancy

- degree ($k$-redundant)

- type
  - hot spare (e.g. 1+1 link redundancy)
  - active load balance
  - on-demand ...

- spatial, temporal, information
**ResiliNets Principles**

**Diversity**

P12: Diversity: provide alternatives

- spatial diversity: topological, geographic
- temporal diversity
- operational diversity
  - implementation (avoidance of monocultures)
  - medium, e.g. fiber and wireless
  - mechanism diversity, e.g. protocol alternatives
ResiliNets Principles
Multilevel Resilience

P13: Multilevel resilience applied to:
- protocol layers (bottom up)
- planes: data, control, management
- components, subnetworks, global internetwork, users
- each level provides foundation for next
ResiliNets Principles

Context Awareness

P14: Context awareness necessary to detect challenges

- resilient components monitor environment
  - traffic, link state, channel conditions, etc.
- necessary to detect adverse event or condition
- prerequisite to adapt behaviour
ResiliNets Principles

Translucency

P15: Translucency to control abstraction between levels
- balance abstraction (opacity) vs. visibility
- between levels (e.g. protocol layers)
- dials instrument from below
- knobs influence from above
ResiliNets Principles

**Behaviour**

- P16: self-organising and autonomic
- P17: adaptable
- P18: evolvable
ResiliNets Principles
Self-Organisation and Autonomicity

P16: Self-organising and autonomic
- auto-configuration, self-organisation (bootstrap)
- self-optimisation, self-management (ongoing)
- self-diagnosis, self-restoration (resilience)
- necessary for resilience with minimal human intervention
  • in systems too complex for humans to fully understand
ResiliNets Principles

Adaptability

P17: Adaptability for detection, remediation, recovery
- short term adaptation to context
- local scope (per node or neighbourhood)
ResiliNets Axioms and Principles

Evolvability

P18: Evolvability for refinement in future behaviour
- long term and larger scope than adaptability
- evolution of network architecture and protocols
ResiliNets Axioms and Principles

Mechanisms

• Mechanisms are used to apply principles
• Examples
  – constraints on protocol operation and network behaviour
  – programmable intelligent network nodes
    • reactive: context aware to react to environment
    • deliberative: planning and reasoning
    • reflective: self-observation and future behaviour modification
  – cross-layer and -plane control loops
  – composable protocols
  – eventual connectivity: store-and-forward; store-and-haul
ResiliNets Axioms and Principles

Methodology

• For each principle
  - apply to particular context, e.g.
    • resilient end-to-end communication
    • resilient routing
    • resilient node architecture
    • resilient compartment
  - many (but not all) principles will apply to each
    • if most are empty then we may have an unnecessary principle
  - either
    • indicate choice (e.g. state)
    or
    • derive mechanism to support
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