INTERNET SECURITY

An Intrusion-Tolerant Approach
from reading assignment 2, the 2006 article by
Y. Deswarte and D. Powell
All material in this sequence was drawn from
the article.

ARPANET

- »What was its main motivation?
- »What faults were considered?
- »What security considerations were considered?

- Limitations
  - malicious attacks & intrusions were not considered, e.g.,
    - no authentication and thus no way to deal with spoofing
    - protocols include network maintenance, e.g., routing

- Attack types
  - e.g., DoS, attacks against confidentiality (get sensitive information), web defacing, ...
- Motivation
  - sport, curiosity, vanity, vandalism, vengeance, greed, political, strategic, ..., terrorism.
- Competence
  - from recreational hacker to specialists
  - criminal, ..., government warfare

- Many ways to attack
  - sniffing, interception (destruction, insertion, modification, replay)
  - address falsifications, injection of counterfeit network control messages,
  - use Internet to find out published exploits
  - ...
  - unknown attack vector

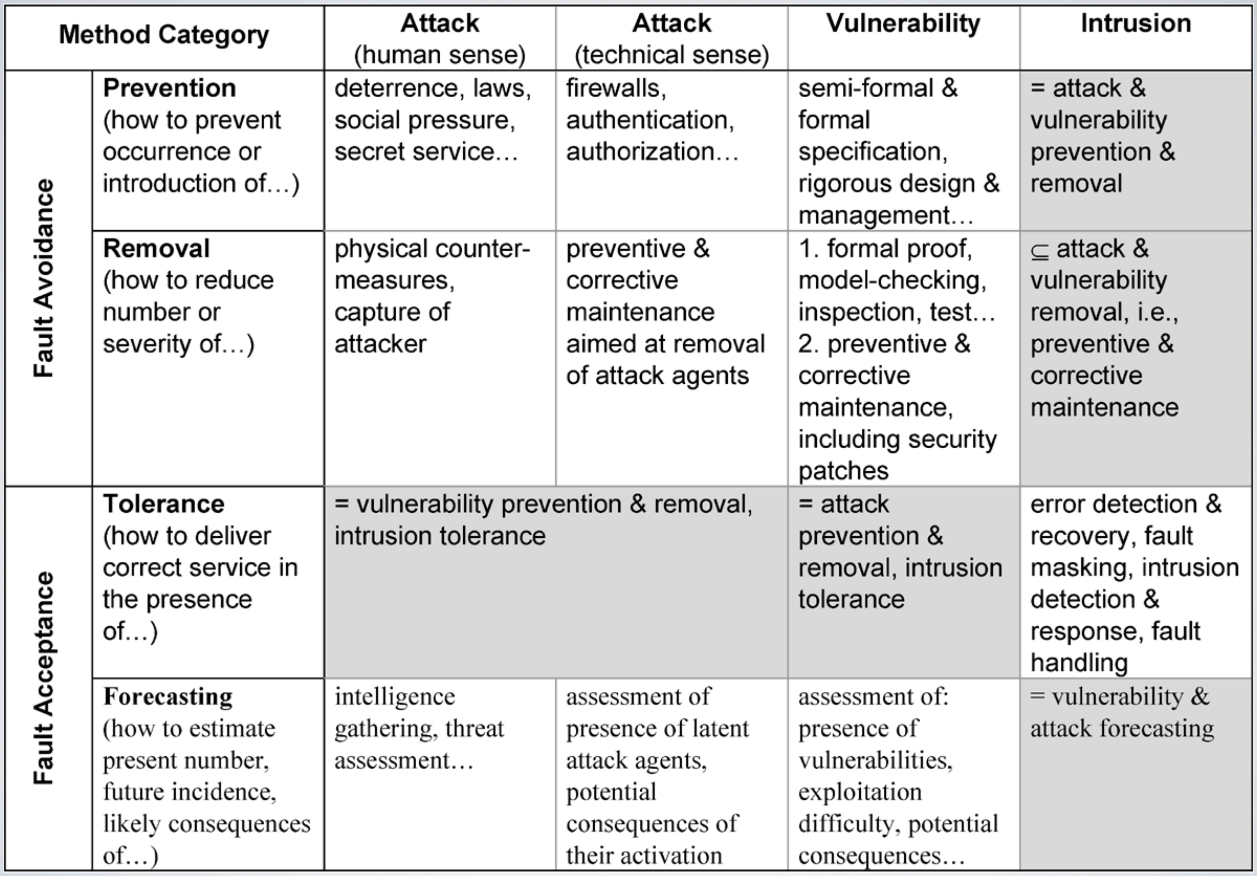
- Conventional security techniques
  - rely mainly on authentication
  - and authorization
    - (least privilege principle)
    - uses detection which aim to detect and block attempts to exceed privileges
  - Does not work in the context of the Internet

- Issues
  - Anybody (even anonymous users) has some rights
  - Many systems are accessible by public
  - COTS OSs are exploitable (due to design flaws etc.)
  - Internet protocols designed when equipment was expensive and intrusions were unlikely (30 years ago)
- Economic pressures of ISPs

- Tolerating malicious act
  - starting in the mid 80s, later projects include
  - OASIS (Organically Assured and Survivable Information Systems)
  - MAFTIA (Malicious and Accidental Fault Tolerance for Internet Applications)

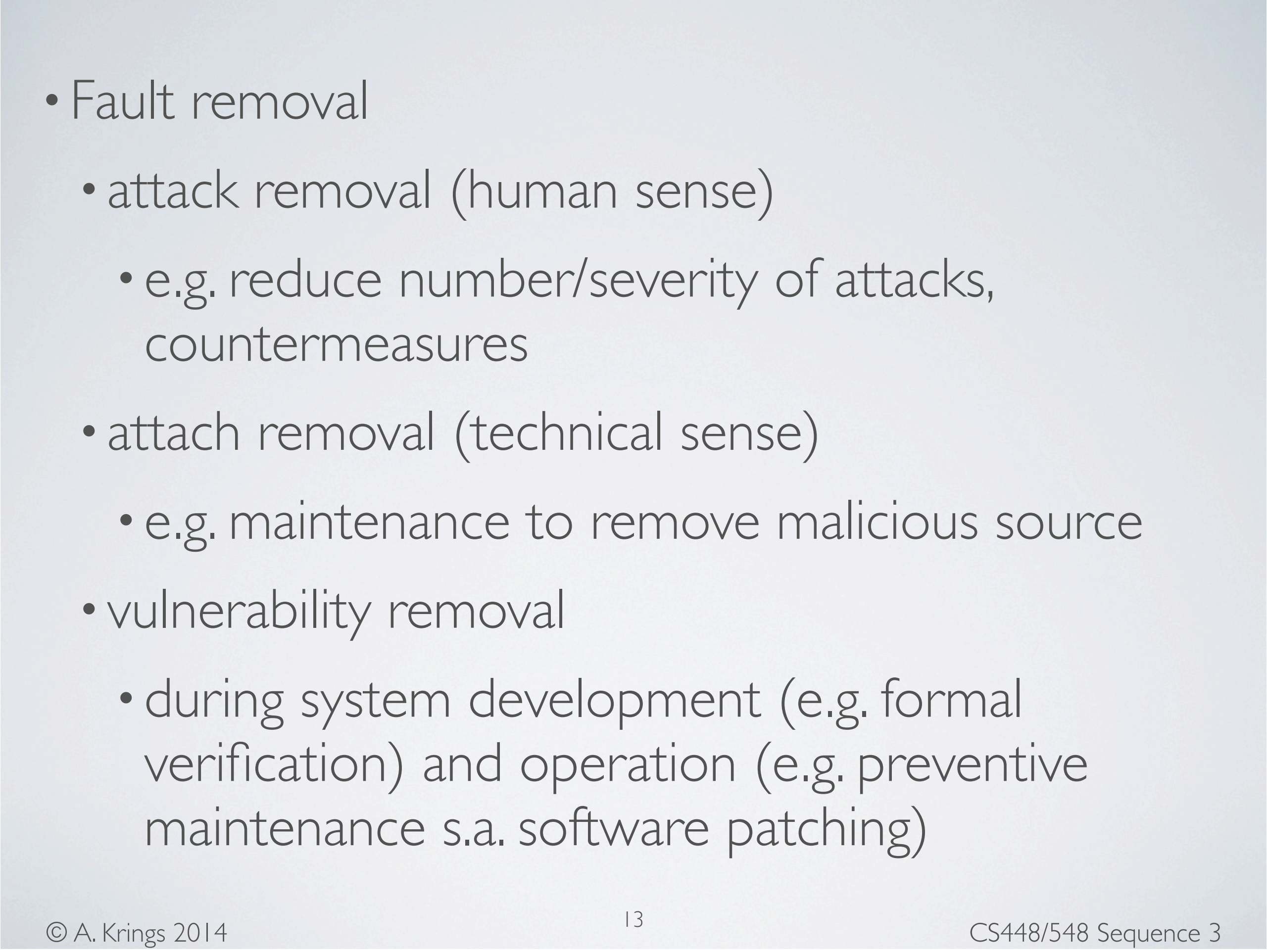
- First key concept from dependability
  - fault > error >failure view Intrusion as a Fault
    - Intrusions as the result of an exploit
    - They argue the error to be the result from an intrusion (fault), which may cause system failure, i.e., violation of system security policy

- Second key concept from dependability
  - fault prevention
  - fault tolerance
  - fault removal
  - fault forecasting
- Fault avoidance (prevention + removal)
- Fault acceptance (tolerance + forecasting)

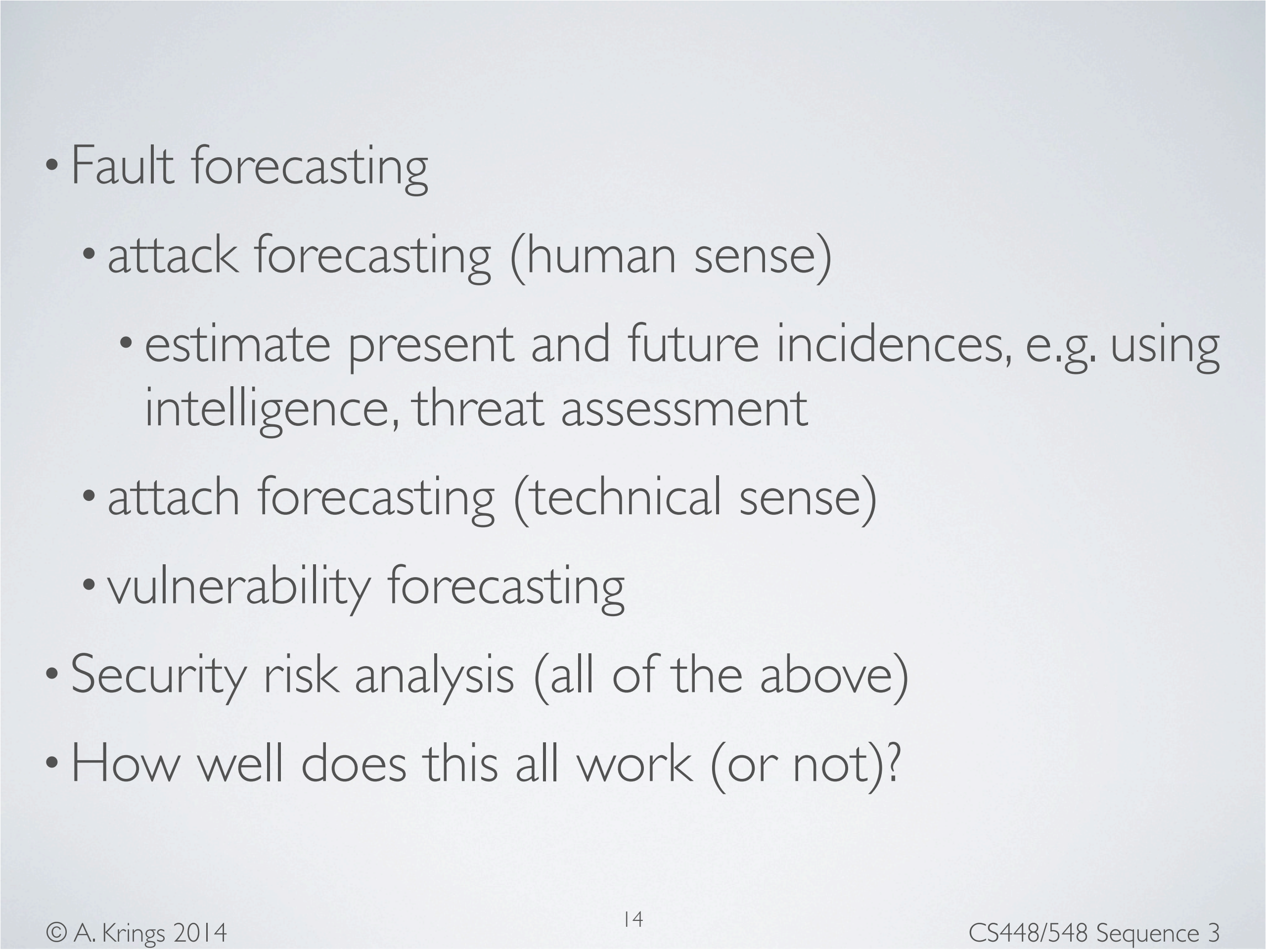


Method Category		Attack (human sense)	Attack (technical sense)	Vulnerability	Intrusion
Fault Avoidance	**Prevention** (how to prevent occurrence or introduction of…)	deterrence, laws, social pressure, secret service…	firewalls, authentication, authorization…	semi-formal & formal specification, rigorous design & management…	= attack & vulnerability prevention & removal
	Removal (how to reduce number or severity of…)	physical counter-measures, capture of attacker	preventive & corrective maintenance aimed at removal of attack agents	1. formal proof, model-checking, inspection, test… 2. preventive & corrective maintenance, including security patches	⊆ attack & vulnerability removal, i.e., preventive & corrective maintenance
Fault Acceptance	**Tolerance** (how to deliver correct service in the presence of…)	= vulnerability prevention & removal, intrusion tolerance		= attack prevention & removal, intrusion tolerance	error detection & recovery, fault masking, intrusion detection & response, fault handling
	Forecasting (how to estimate present number, future incidence, likely consequences of…)	intelligence gathering, threat assessment…	assessment of presence of latent attack agents, potential consequences of their activation	assessment of: presence of vulnerabilities, exploitation difficulty, potential consequences…	= vulnerability & attack forecasting

- Fault prevention
  - attack prevention (human sense)
    - e.g. deterrence
  - attach prevention (technical sense)
    - security mechanisms
  - vulnerability prevention
    - e.g. applying good software engineering practices (from formal specifications to education)



- Fault removal
  - attack removal (human sense)
    - e.g. reduce number/severity of attacks, countermeasures
  - attach removal (technical sense)
    - e.g. maintenance to remove malicious source
  - vulnerability removal
    - during system development (e.g. formal verification) and operation (e.g. preventive maintenance s.a. software patching)



- Fault forecasting
  - attack forecasting (human sense)
    - estimate present and future incidences, e.g. using intelligence, threat assessment
  - attach forecasting (technical sense)
  - vulnerability forecasting
- Security risk analysis (all of the above)
- How well does this all work (or not)?

- Intrusion tolerance
  - organize and manage a system such that an intrusion in one part of the system has no consequence on its overall security.
  - common mode faults: same type of attack succeeds in different parts of the system
  - confidentiality: intrusion in one part of the system should not reveal confidential data

- Tolerance based on intrusion detection
  - Intrusion detection techniques
    - don’t detect intrusions, but their effects
    - anomaly detection
    - misuse detection

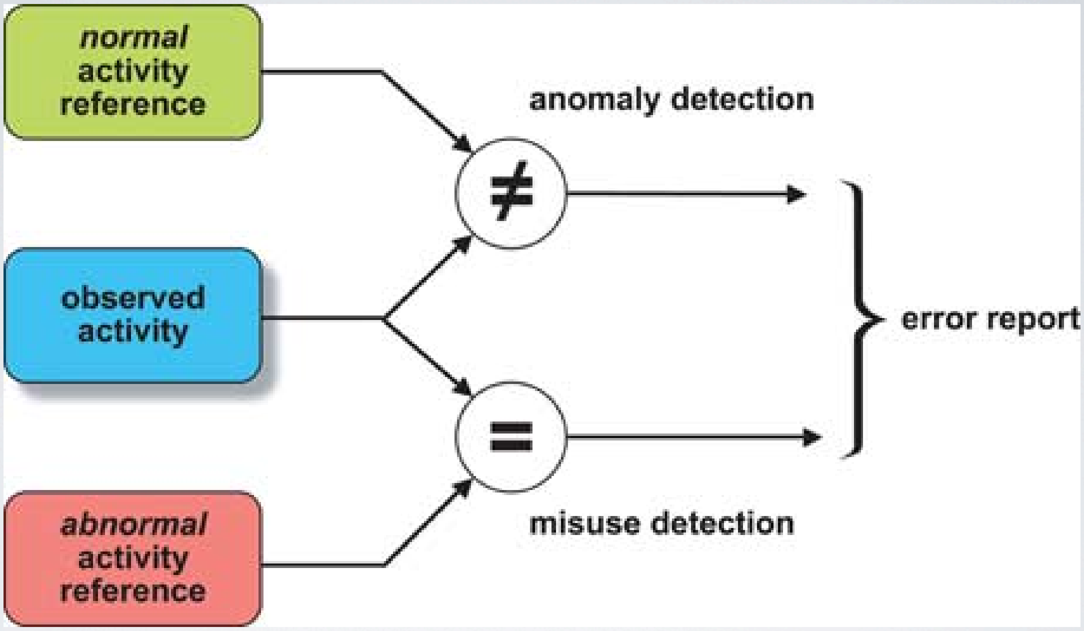


Fig. 1. Intrusion detection paradigms.

- FRS Fragmentation Redundancy & Scattering
  - Fragmentation: split sensitive data into fragments
  - Redundancy: without redundancy no recovery after data corruption/loss, perhaps not even detection.
  - Scattering: topological, geographic, temporal. Applies also to separation of duty (no centralized control)
  - FRS used in Delta-4 project

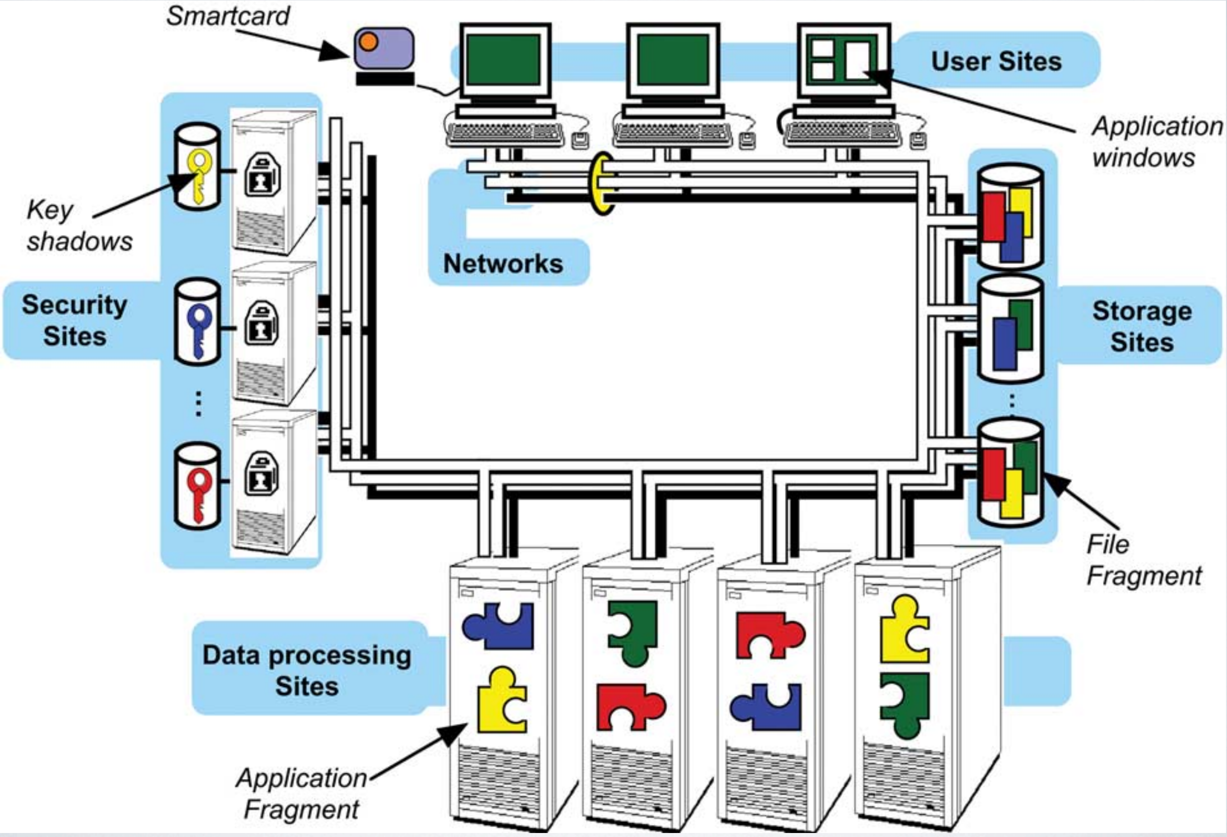
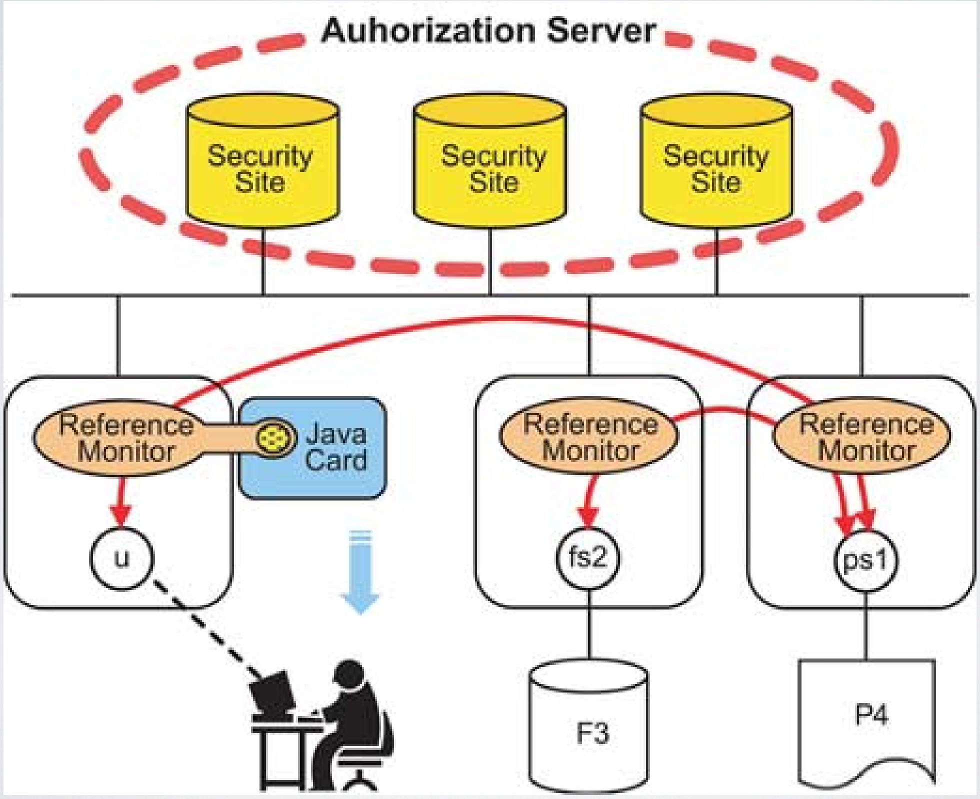


Fig. 2. FRS in Delta-4.

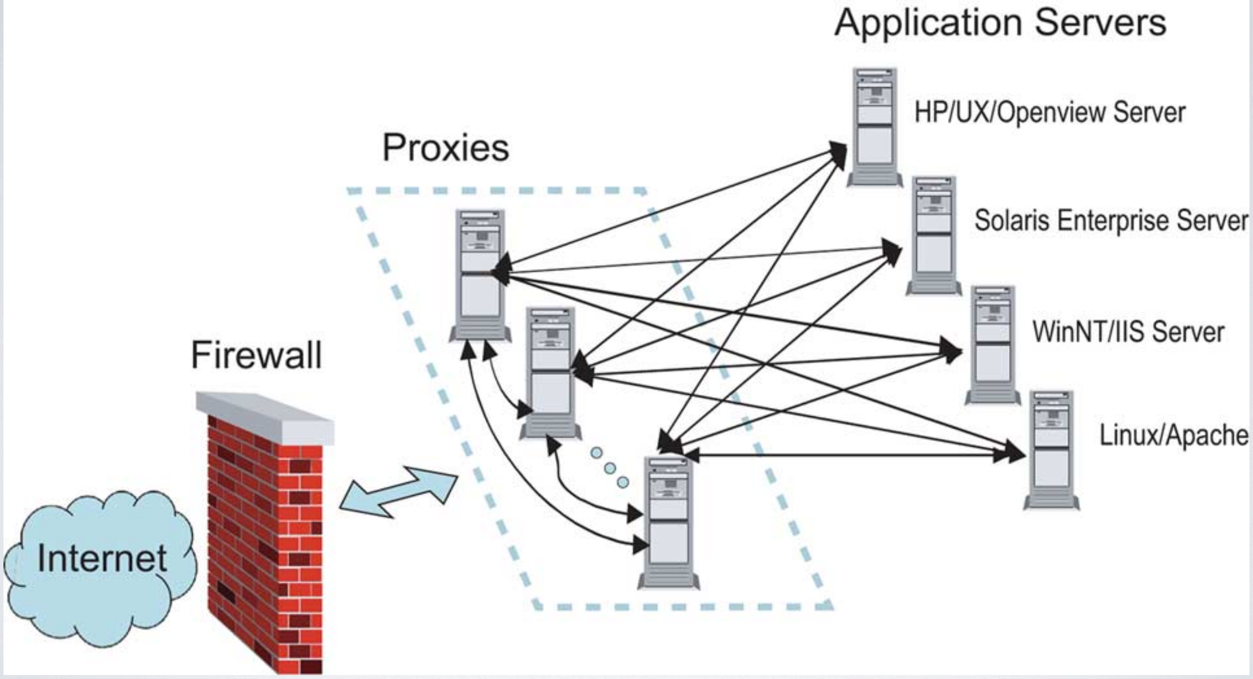
- MAFTIA
  - attempt at intrusion-tolerant Internet applications
  - we will look at this later in detail
  - one issue is that the intrusion detection mechanism must be made intrusion tolerant itself

- MAFTIA authentication scheme



- DIT (Dependable Intrusion Tolerance) architecture
  - web server that continues to provide correct service in the presence of attacks
  - diversification to avoid common mode fault
  - servers isolated from Internet by proxies

- DIT architecture



- Summary
  - this was another general article pointing out general principles that will help towards building systems that can tolerate maliciously induced faults