

Reti senza IP

titolo ad effetto per chiaccherare di tecnofilosofia

Rete: caso/cosa in cui i link valgono di piu' degli elementi.

cosa non del tutto scontata, ad esempio, dove il riso è la moneta di scambio... vale di più l'elemento riso, che il contatto con il risaiolo...

```
vecna – moca 0x7D8/hackmeeting 3730 http://www.delirandom.net
```

```
pub 1024D/602EEFA5 2007-08-28 [expires: 2009-08-27]  
Key fingerprint = B9B6 AE8A F4BC 3261 FD1F 70AF 16F0 9BEA 602E EFA5  
uid          vecna <vecna@winstonsmith.info>  
uid          vecna <vecna@delirandom.net>  
uid          vecna <vecna@s0ftpj.org>
```

Antefatto...

Nel 1993, John Arquilla & David Ronfeldt, nel RAND, scrissero “the advent of netwar” ...

La sua lettura risultò illuminante una volta comparata con gli eventi che scuotevano l'Internet

Nonostante cercasse di rispondere alla domanda: “gli US quali vantaggi/svantaggi possono avere dalla rete ?”

Questi spararono una filippica che partiva dal neolitico...

Storiella delle forme organizzative, 1

FORMA TRIBALE:

Periodo Neolitico, la linea di discendenza è la forma di elezione a centro di potere, l'obiettivo di questa forma è la sopravvivenza, l'appartenenza e l'identità. La sua forza è nel consolidare una cultura di base e condivisa all'unanimità, la sua debolezza la scarsità di potere derivato dal numero di elementi limitato e la centralizzazione totale diminuisce il numero di aspetti che possono essere amministrati dal re/dal capo.

Manifestazioni di questa forma si rivedono in:
dinastie, mafia, gang urbane, diaspora.

Storiella delle forme organizzative, 2

FORMA GERARCHICA:

Impero Romano, papato e assolutismo le prime forme di organizzazione gerarchica, l'obiettivo diventa il potere, l'amministrazione e l'espansione, la forza è rappresentata dai contributi fisici, monetari e informativi che gli elementi della piramide possono dare, la debolezza sta nella lentezza con la quale i vertici della piramide riescono a controllare le proprie basi, pertanto situazioni che richiedono velocità e dinamismo, come il mercato o l'interazione con altre gerarchie, il processo risulta molto limitato.

Storiella delle forme organizzative, 3

FORMA MERCANTILE/BASATA SUL MERCATO:

Il mercato nel senso locale del termine esiste dal tempo dei greci, ma l'arte mercantile della vendita che sfrutta le differenze ambientali e culturali per importare ed esportare prodotti è iniziata nell'alto medioevo per avviarsi definitivamente tra il 17 e il 18 secolo. La base di questa forma organizzativa è la competizione e l'indipendenza, l'assenza di un'ideologia ma di un obiettivo a breve termine. e' diventato la base per la creazione di sistemi gerarchici e tribali sempre focalizzati al mercato.

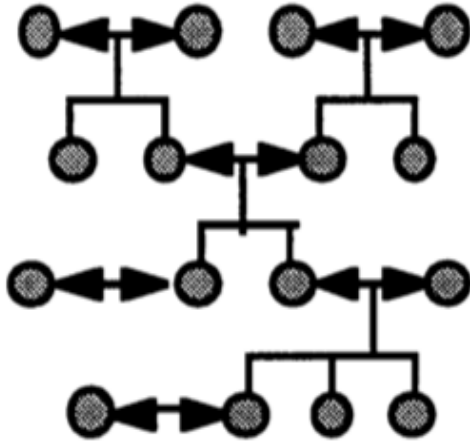
Storiella delle forme organizzative, 4

FORMA A RETE DISTRIBUITA:

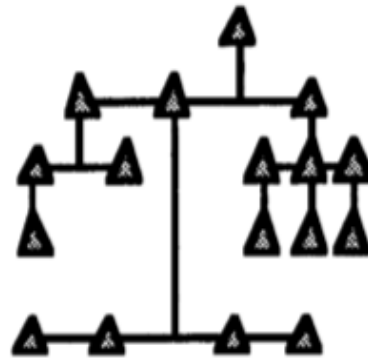
nuovo modello organizzativo, nato nell'era della comunicazione globale, strutturata da una collaborazione eterogenea, che mira ad una sorta di equità e condivisione. Realizzazione di obiettivi comuni, valorizzazione delle differenze in quanto apporto di caratteristiche diverse all'interno del gruppo. Velocità di aggregazione e dinamicità nell'azione. La debolezza sta nell'incostanza e nell'eccessiva dinamicità.

Storiella delle forme organizzative, 5

PRIMA FORMA:
Organizzazione basata sulla famiglia allargata e rapporti di parentela.



SECONDA FORMA:
gerarchica istituzionale, ancora presente in chiese/eserciti



TERZA FORMA:
mercato libero, ogni individuo cerca di dare il meglio di se organizzandosi indipendentemente, da lui possono dipendere micro-gerarchie.



QUARTA FORMA:
rete distribuita: ogni elemento è indipendente e trova i suoi complementari per un fine comune



Storiella delle forme organizzative, 6

	Tribale	Gerarchica	Mercato	Rete distribuita
Era	primitiva	agricola	industriale	post-industriale
Reame	famiglia	governo	economico	società civile ?
Interessi	identità	autorità	soldi	conoscenza ?
Valori	appartenenza	ordine	libertà	giustizia ? equità ?
Rischi	nipotismo (?)	corruzione	sovversione	infiltrazione
Prodotto (beni):	familiari	pubblici	privati	collettivi
Motivazione	sopravvivenza	autorità	egoismo	consenso
Limiti	decisioni	controllo	commerciale	equità sociale / caos
Architettura	labirinto	piramide	atomi	gomitoli
Metafora fisica	pelle	scheletro	circolatorio	nervoso
Tecnologia	simboli	scrittura	telegrafo	comunicazione digitale

2+2 ...

1) la forma distribuita dimostrava i suoi vantaggi: dinamicità, capacità adattive, efficienza

2) le forme più centralizzate mostravano degli svantaggi intrinseci: incertezza di imparzialità, corrottile, supervisore totale

... come in Internet !?

= se le applicazioni migrassero il più possibile verso una distribuzione a rete ?

In internet possiamo generalizzare con 3 forme di riferimento

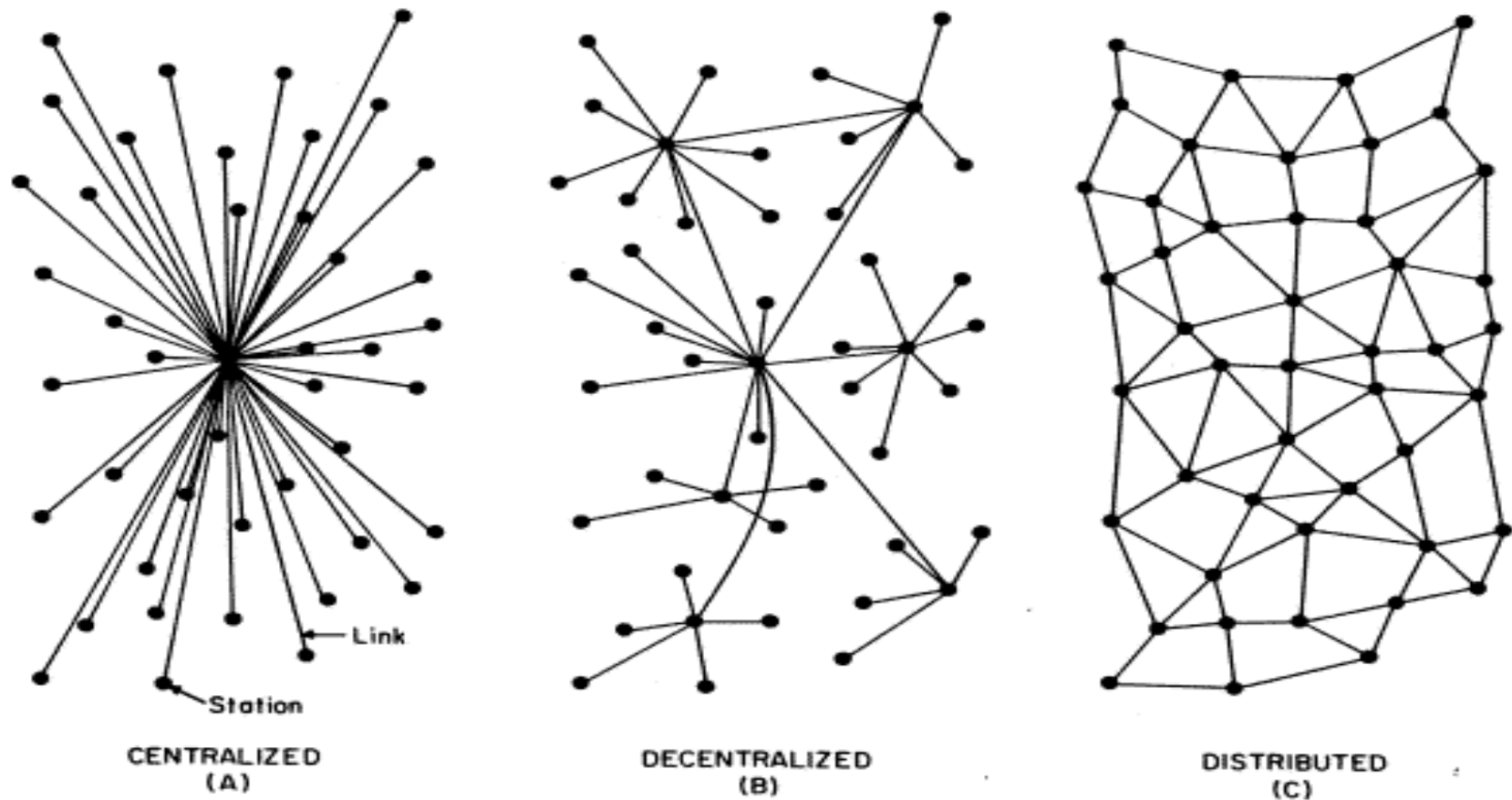


FIG. 1 - Centralized, Decentralized and Distributed Networks

E possiamo generalizzare **3 forme di attacco:**

Controllo

lettura dei dati in transito, sia di contenuto che di protocollo.

Negazione

blocco o isolamento del servizio, totale/parziale, selettivo/massivo

Deception (sovversione ? disvio ?)

iniezione di dati falsi al fine di influenzare l'elemento destinatario.

Ogni “cosa” può avere una propria analisi dal punto di vista dei suoi link (va poi aggiunta l'analisi dei layer!)

Youtube: sistema centralizzato

*mule: decentralizzato

freenet: distribuito

TOR: distribuito

IRC: decentralizzato

IM privati closed (MSN/Gtalk): centralizzati

Skype: decentralizzato/distribuito (closed)

GnuNet: distribuito (open)

Jabber + OTR

DNS: decentralizzato

Routing IP: decentralizzato

Come si concretizzano gli attacchi ?

Youtube: censura, profilazione,

*mule: distribuzione fake, controllo lato server, sequestri

freenet: (nessuno ?)

TOR: distrib DoS (non nel senso di mixer)

IRC: sniffing, fake/emulazione, sequestri/dos

MSN/Gtalk: profilazione, blocco utenti

Skype: idem come sopra + olio di serpente

GnuNet: (nessuno ?)

Jabber + OTR: DoS/compromissione/sequestri

DNS: censura, profilazione, spoofing

Routing IP: censura, profilazione, hijacking

La stratificazione delle reti (ISO/OSI)

Layer 1/Elettrico:
Rete decentralizzata

Layer 2/Ethernet:
host immediatamente
connessi tra loro
(hub/switch e loro !=)

Layer 3/Rete:
Rete decentralizzata per
segmenti e ISP

Layer 4/Trasporto:
Servizi esposti tra hosts

Layer 5-7/...
Dati trasmessi e
visualizzati

Layer 8/umani-altro ?
Entità che si scambiano
dati

Ad ogni singolo livello ISO/OSI, puo' avvenire N/C/D

1/Elettrico	N:(corrente spenta) C:(profilazione consumo)
2/Ethernet	N/C/D:(arp hijacking/port monitor/sniffing)
3/IP	N:(routing) C:(router) D:(hijacking)
4/UDP/TCP	N:(RST) C:(servizio) D:(hijacking del servizio)
5-7	N:(DoS) C:(flussi dei dati) D:(creazione dei dati)
8	N:(r.i.p.) C:(attacchi fisici/OSI) D:(raggiro/SE)

Questo ci puo' dare una visione piu' analitica delle vulnerabilità
“architetturali” e prevederle/exploitarle

Se c'è protezione, gli attacchi (C/D) a layer inferiore perdono importanza

1) Attacchi ethernet/IP: lo sniffing/l'hijacking perdono di importanza se proteggo il traffico

1a) *reti wifi aperte, attacchi arp *, attacchi con tunnel.*

2) Attacchi TCP/Applicativi: la deception perde di importanza se firmo il traffico

2a) *phishing, fake/emulazione di identità*

3) (alcuni) attacchi di N/C/D perdono importanza se anonimizzo mittente/destinazione

3a) *censura, sequestro, controllo, attacchi, ecc...*

i flussi informati(vi|ci) in una direzione piu'
distribuita, 1

Che non abbia punti deboli attaccabili con:

controllo/profilazione (e controllo di tutti gli utenti connessi)

negazione/censura (interruzione di tutto il servizio)

decepcion/disinformazione (raggiro di tutti gli utenti).

Distribuendo si elimina il punto vulnerabile.

i flussi informati(vi|ci) in una direzione piu'
distribuita, 2

La crittografia a chiave pubblica garantisce riservatezza e identificazione (anche anonima)

Immaginiamo che i giornalisti, una volta emessa la firma digitale del loro articolo, non possano più vederlo modificato

Immaginiamo che ogni scambio di mail non transiti per dei server intermedi, ma direttamente verso l'utente

**Perchè avvenga la distribuzione, l'”intelligenza”
deve essere su ogni client.**

i flussi informati(vi|ci) in una direzione piu' **distribuita, 3**

Qualunque scambio di dati puo' essere reso serverless
(posta, web, chat)

kazaa/skype hanno fatto scuola: ogni client si comporta in modo indipendente, i client che piu' hanno banda, hardware e presenza popolano piu' cache cosi' da essere eletti dinamicamente ad un ruolo simile a quello di server.

L'attacco alle reti p2p e le sue difese

Il fatto che tutti abbiano la stessa importanza è stato sintomo di abusi nelle reti p2p

La mancanza di autorità NON deve significare mancanza di autorevolezza

l'autorevolezza si è incarnata in: commenti TPB/ed2k, feedback ebay, digg e sistemi di filtro collaborativo, web of trust (blog/rss)

La semplicità della centralizzazione

La “visione” di Google è stata: “gli utenti avranno bisogno di qualcuno a cui affidarsi, e a quel qualcuno volenti o nolenti daranno i loro dati”.

= Google ha vinto :)

Ogni elemento (de)centralizzato che ci offre dei servizi, ha i nostri dati in cambio.

L'unica alternativa è che la progressiva forma distribuita, è trovare feature che valorizzino questa forma

Successi e insuccessi della distribuzione, 1

Napster e la falsa distribuzione (file sharing via irc)

Anonymous remailer come decentralizzazione poco rilevante

TOR e la debolezza del directory server

la vittoria di KAD(U)

La triste storia di all-peers

Successi e insuccessi della distribuzione, 2

I requisiti della collaborazione:

IP pubblico + sistemista + conoscenza + costanza

voglia + conoscenza + spazio web php/mysql

spazio web php/javascript + conoscenza

plugin per firefox

Cronaca

1. Project Chanology (anonymous vs 1)
2. Sex crimes & Vatican (centralizzazione MM)
3. Media defender – defender (anonymous vs 1)
4. (h0n0/b4b0/InternetSuperHeros) vs ITSec (anon vs *)
5. R*, 95%, SmallSister
6. TelecomItalia/TelecomGrecia/TelecomGermania (biz)
7. Fantasia web contro la censura (rapidità della rete)
8. Estonia & Cina & netwar (* vs *)

Conclusione

Voglio solo darvi una visione :)

Vedere ogni elemento come un atomo di una rete, vedere se un flusso è leggibile ed a chi, e se lascia dati correlabili o meno.

Questa visione consente di razionalizzare le debolezze architettoniche, per individuare più rapidamente le vulnerabilità di un sistema, informati(co|vo), finanziario, sociale.

NON ABUSARNE :)

Candy Mountain!

Nessuna domanda =
Rileggete le slide.

DOMANDE ?