

La Sicurezza ICT e la difesa del patrimonio informativo



DICO

Danilo Bruschi

Dip. di Informatica e Comunicazione

Università degli Studi di Milano

bruschi@dico.unimi.it



DICo

Argomenti Trattati



- Un po' di storia
 - Le reti di comunicazione
 - Le tecnologie dell'informazione
- L'insicurezza delle ICT
 - Vulnerabilità
 - I rischi
 - Le minacce
- Le contromisure
 - Tecnologiche
 - Organizzative
 - Socio-Politiche
- Scenari evolutivi

Un pò di storia ...



DICo





DICo

Un po' di storia ...

- A metà degli anni '60 il DoD dà vita al progetto ARPANET
- rete di controllo che potesse sopravvivere ad una guerra nucleare
- la resistenza ai guasti è garantita dalla natura punto-a-punto con ridondanza di cammini
- la rete è di uso esclusivo militare e di ricerca

Un po' di storia ...



DICo

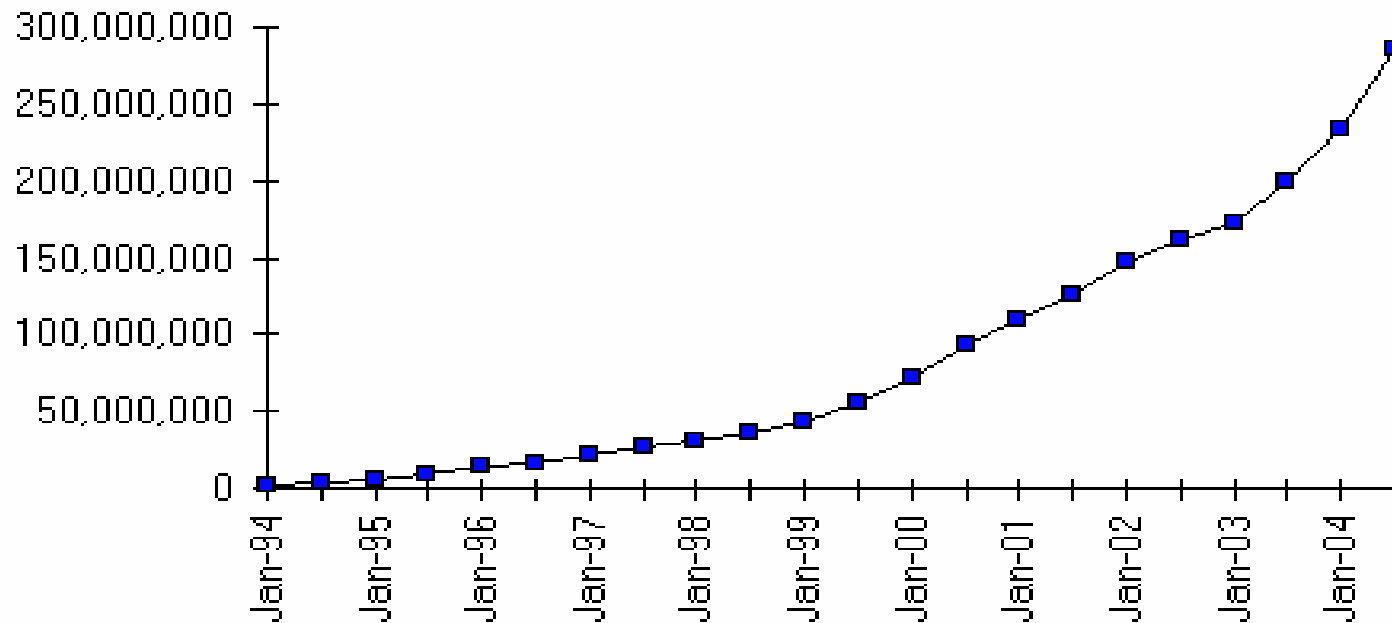
- Dicembre 1969 - UCSB, UCLA, SRI, Utah
- Marzo 1971 – 15 Nodi
- 1983 - viene separata la MILNET
- 1990 - integra NSFNET, BITNET, HEPNET, SPAN, EARN
- 1990 - ARPANET viene smantellata, ormai sostituita da Internet

Oggi



DICo

Internet Domain Survey Host Count



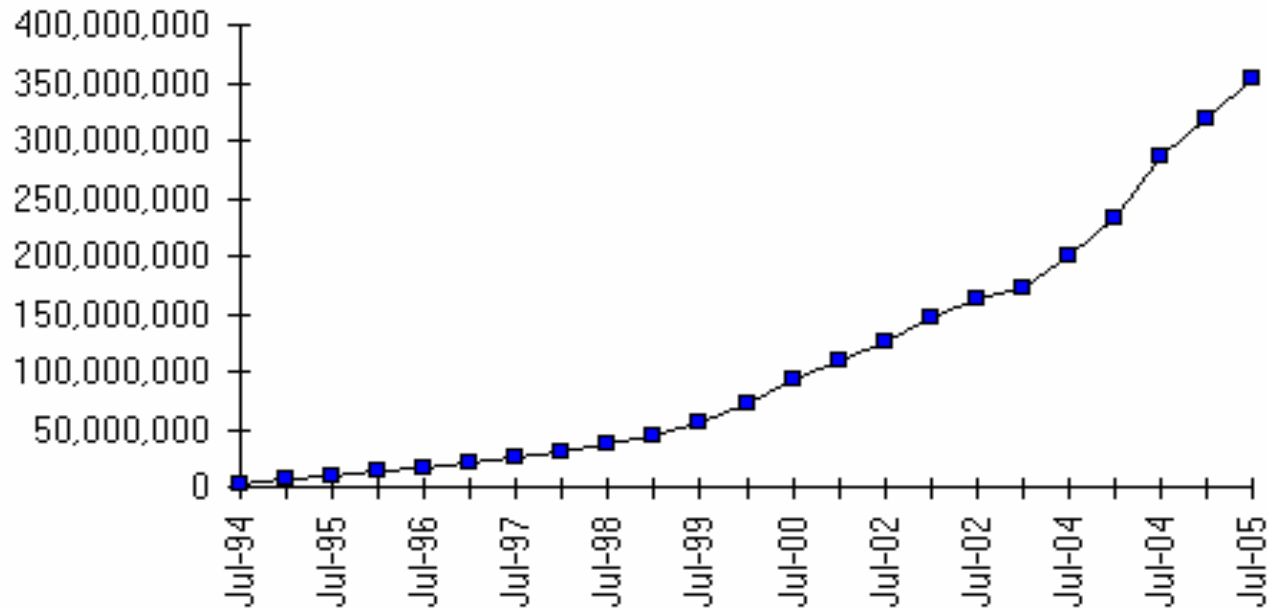
Source: Internet Software Consortium (www.isc.org)

Oggi



DICo

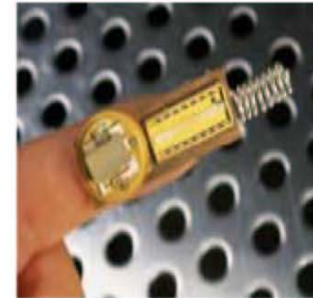
Internet Domain Survey Host Count



Source: Internet Software Consortium (www.isc.org)

Internet domani

- Miniaturized **cameras**, microphones,...
 - **pattern recognition**, assisted by heuristics
 - speaker recognition, **speech controlled** devices
- **Fingerprint** sensor on mobile objects
- **Radio sensors**
 - without power supply
- **Location sensors**
 - e.g., based on GPS
- **Dust sensors**



POSITION
N 47°
23'17"
E 008°
34'26"

F. M. 00

Source: F. Mattern, 2001

Internet domani



DICo

NET FRIDGE

LG Electronics Digital DIOS Internet Refrigerator

LG Electronics recently unveiled an Internet-enabled LG-brand refrigerator, microwave oven, and washing machine for U.S. consumers. These next-generation appliances will communicate with each other via a digital home network and will leverage the power of the Internet for the comfort and convenience of the consumer.

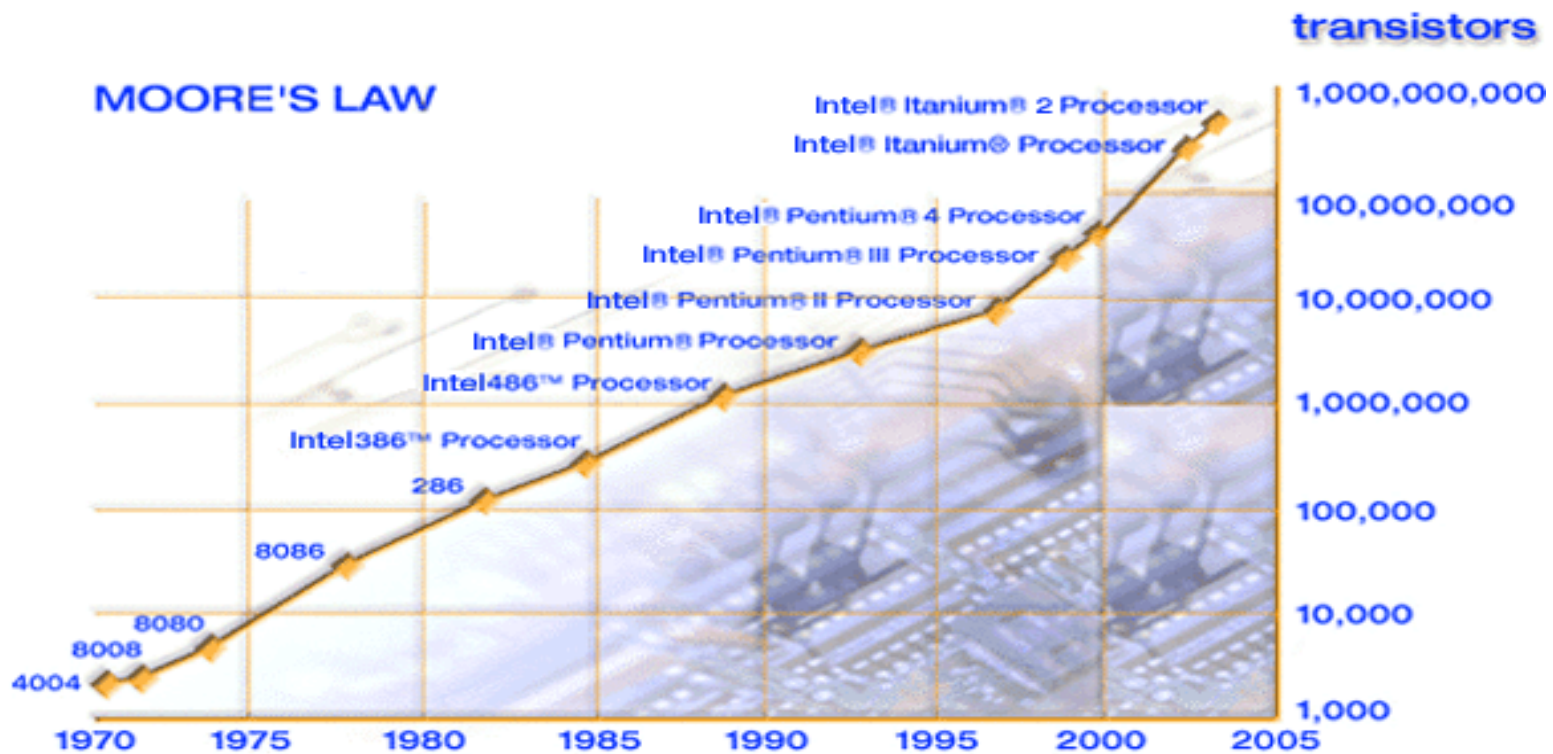


Internet Refrigerator

La legge di Moore



DICo





DICo

I Sistemi di memorizzazione

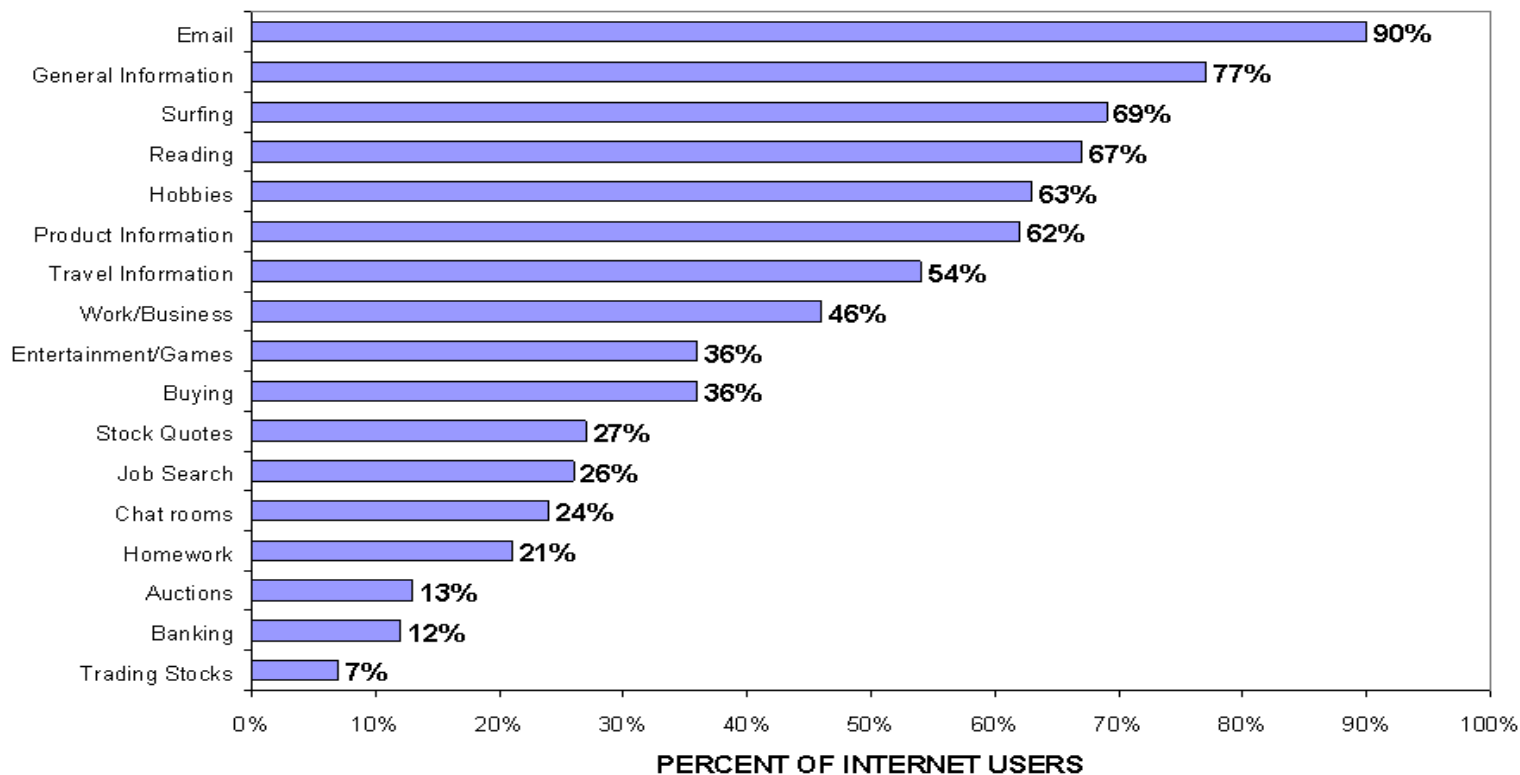
- La densità delle DRAM aumenta del 40-60% all'anno
- La banda è aumentata del 66% in 10 anni, la banda
- La densità dei dischi aumenta del 100% ogni anno

Di fatto oggi la rete è ...



DICo

WHAT USERS DO ON THE INTERNET





DICo

Argomenti Trattati

- Un po' di storia
 - Le reti di comunicazione
 - Le tecnologie dell'informazione
- L'insicurezza delle ICT
 - Vulnerabilità
 - I rischi
 - Le minacce
- Le contromisure
 - Tecnologiche
 - Organizzative
 - Socio-Politiche
- Scenari evolutivi





DICo

Sicurezza Informatica

Che cos'è un sistema informatico sicuro?

- Un sistema che comunque usato (intenzionalmente o in modo non autorizzato) non provoca alcuna conseguenza avversa e che è in grado di rilevare tempestivamente tentativi di intrusione



DICo

... e la sicurezza?

1987

- Viene arrestato ad Hannover uno dei più famosi hacker della storia: Matthias Speer (pseudonimo)
- In due anni di attività riesce a violare l'accesso ad alcune decine di host e reti, tra cui diversi siti di basi militari USA,
- Viene catturato mentre scarica alcuni file, opportunamente predisposti dalla FBI, che apparentemente contengono informazioni in merito al progetto "Guerre Stellari"

... e la sicurezza?



DICo

2 Nov. 1988

Robert Morris uno studente di Ph.D della Cornell University mette fuori causa, nell'arco di poche ore, 6000 computer connessi a Internet



DICo

Intrusioni (2)

Giugno- Ottobre 1994

intrusori Russi acquisiscono password di utenti dei sistemi della CITIBANK e tentano il trasferimento di \$10M su conti personali

- la banca perde \$400,000
- 2 arresti negli U.S.A.
- 1 condannato in Israele
- 1 arresto in Netherlands
- il principale protagonista, Vladimir Levin, viene condannato a 36 mesi di carcere

Intrusioni (3)



- Dopo il licenziamento dalla Forbes, George Parente si connette da casa ai sistemi della Forbes e mette fuori uso 5 network server
- Il danno ha provocato due giorni di inattività per l'azienda, per un ammontare di circa \$100,000



DICo

Vulnerabilità di un sistema

- Tecnologie
 - Errori di progettazione
 - Errori di implementazione
 - Errori di configurazione
- Processi
 - Errori di progettazione
 - Bad practices



DICo

Rischi

- Perdita d'immagine verso l'opinione pubblica
- Perdita d'immagine verso i propri clienti
- Perdita del competitive advantage
- Furto di Informazioni sensibili
- Blocco di attività critiche
- Mancato rispetto di regole contrattuali
- Coinvolgimento in procedimenti processuali
- Danneggiamento degli asset

Chi?



- Non Strutturati
 - Insider, Ricreational Hackers, Hackers “Organizzati”
- Strutturati
 - Crimine organizzato, Spionaggio industriale, Terroristi
- National Security
 - Intelligence, Information Warriors



DICo

Argomenti Trattati

- Un po' di storia
 - Le reti di comunicazione
 - Le tecnologie dell'informazione
- L'insicurezza delle ICT
 - Vulnerabilità
 - I rischi
 - Le minacce
- Le contromisure
 - Tecnologiche
 - Organizzative
 - Socio-Politiche
- Scenari evolutivi



La Risposta



- E' possibile difendere con probabilità di successo estremamente elevate la propria rete dalle intrusioni, è necessario però intraprendere le opportune misure che devono essere sia di natura ORGANIZZATIVA che di natura TECNOLOGICA



DICo

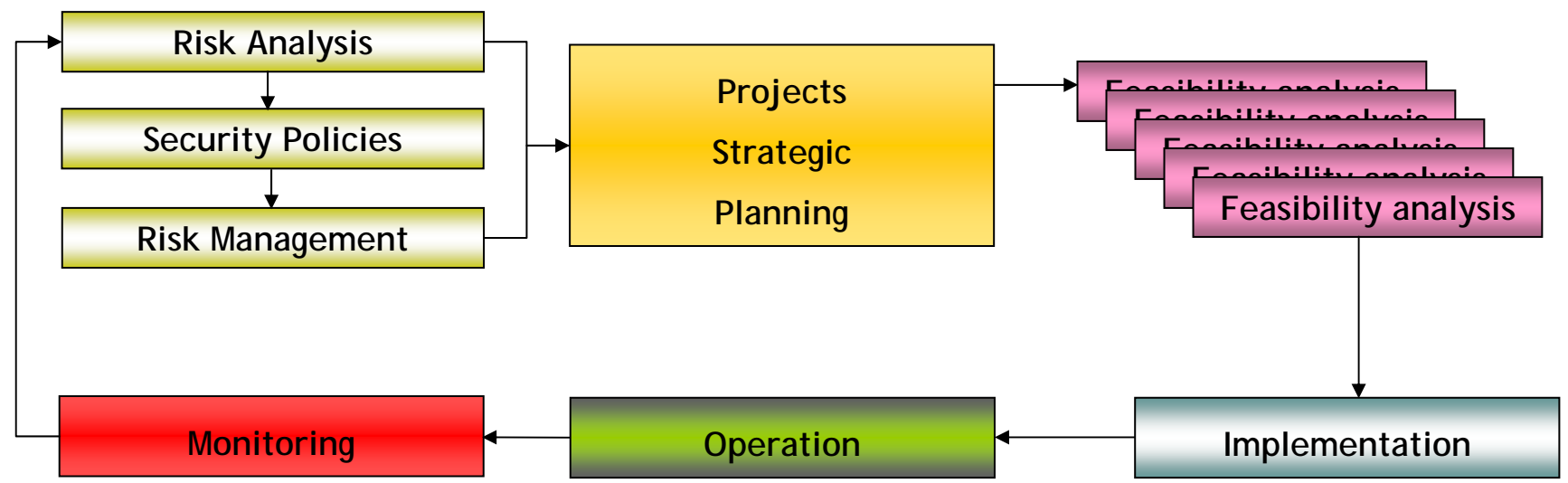
Contromisure Organizzative

- Analisi dei rischi
- Politiche per la sicurezza
- Gestione del rischio
- Audit
- Formazione
- Condivisione delle informazioni
- Programmi di formazione per gli utenti
- Infrastrutture organizzative



DICo

Security designing life-cycle





DICo

ROI

- **Risparmi nelle aree:**
 - Incident recovery
 - Business continuity
 - Downtime recovery
- **Minori perdite dati**
- **Salvaguardia dell'immagine dell'azienda**
- **Riduzione downtime**
- **Razionalizzazione della struttura organizzativa**



DICo

I primi strumenti

- A partire di primi anni '90 fanno la loro apparizione i primi strumenti di protezione:
 - Antivirus
 - Firewall
 - Host/Network Scanner
 - Crittografia
 - Strong authentication
 - Firma digitale
 - Kerberos



DICo

Gli strumenti di II Generazione

- A cui fanno seguito:
 - IDS (Intrusion Detection System)
 - PKI (Public Key Infrastructure)
 - VPN (Virtual Private Network)
 - Tecniche biometriche
 - IPSEC/SSL
 - Business continuity
 - Metodologie



DICo

Gli Strumenti di III Generazione

- Log Consolidation
- Event correlation
- Managed Security Service
- Alert System
- Threat Management System
- Identity Management
- DRM
- Content Filtering



DICo

Iniziative del Governo

- **Direttiva sulla sicurezza ICT**, emanata con direttiva del Presidente del Consiglio dei Ministri 16 gennaio 2002;
- **Comitato Tecnico Nazionale sulla Sicurezza ICT**, istituito con Decreto Interministeriale del Ministro delle Comunicazioni e del Ministro per l'Innovazione e le Tecnologie nel luglio 2002, che ha il compito di raggiungere i seguenti obiettivi:
 - esame della situazione della PA rispetto ai temi della sicurezza;
 - elaborazione e diffusione di linee guida;
 - stesura di progetti di attuazione dei principi fissati



DICo

Iniziative del Governo

- **Osservatorio per la sicurezza delle reti e la tutela delle comunicazioni:** istituito dal Ministro delle Comunicazioni di concerto con il Ministro della Giustizia e il Ministro dell'Interno, nel Gennaio 2003
- **Comitato di Garanzia Internet e Minori:** istituito dal Ministro delle Comunicazioni di Concerto con il Miinistro per l'Innovazione e le Tecnologie, nel Febbraio 2004



DICo

Conclusioni



“There is no security on this earth, there is only opportunity.”

(Gen. D. Mc Arthur)