



Berner Tagung für Informationssicherheit 2000  
Sicherheitsfaktor Mensch: Chancen und Risiken

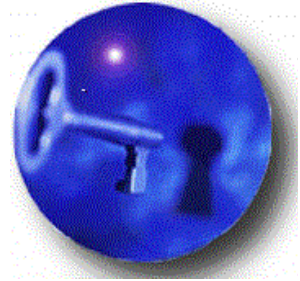


## **Wie gehen Anbieter mit dem Sicherheitsfaktor Mensch um?**

Matthias Kaiserswerth  
IBM Zurich Research Laboratory  
kai@zurich.ibm.com

14.11.2000





# Agenda

- E-business Outlook
- Internet Security Challenge
  - What are we up against?
  - What can we do about it now?
- What is the future?
  - Secure operating systems
  - Secure hardware
  - Intrusion and fraud detection





# e-business:

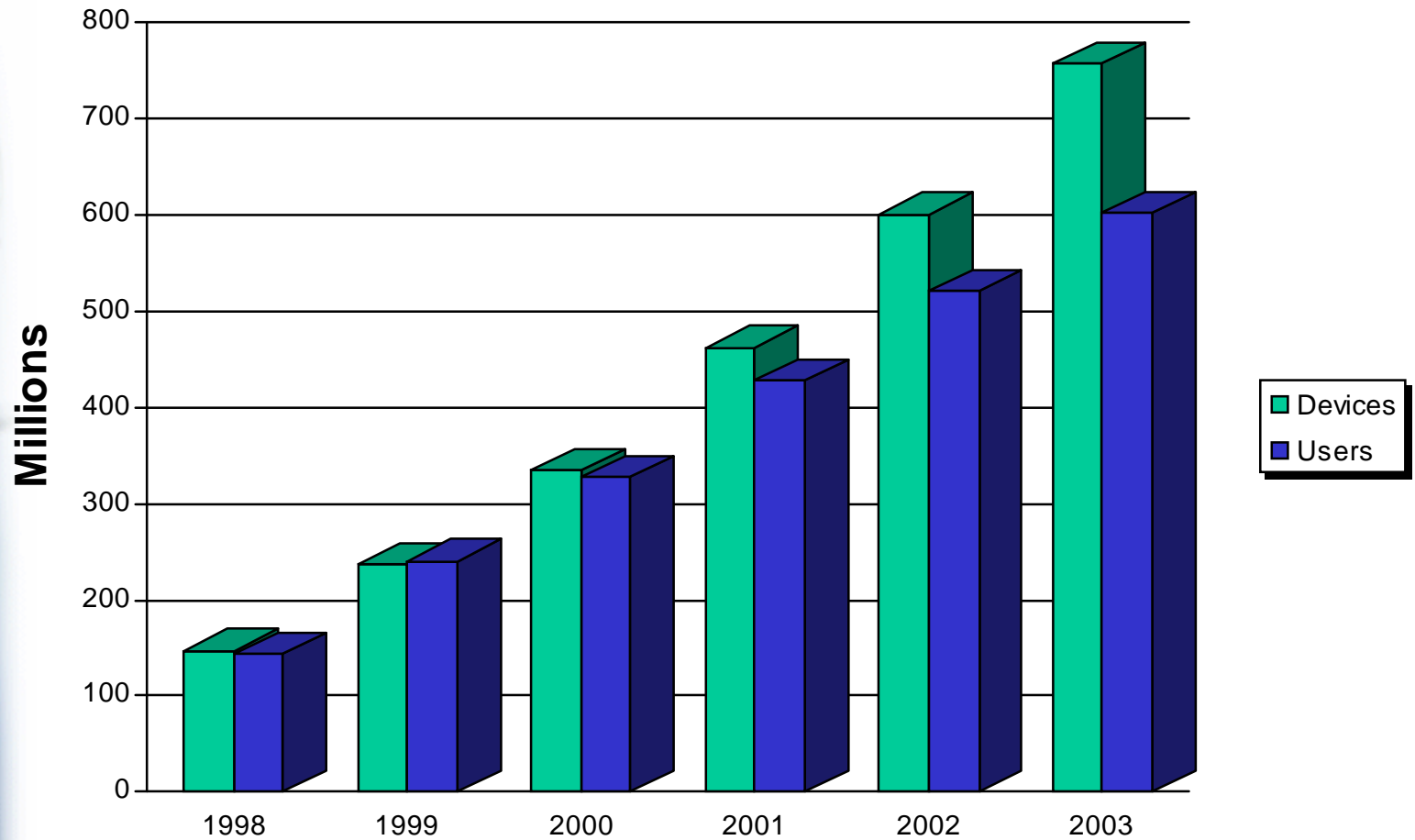
## Business as Usual in Extraordinary Ways

- Global reach
- Information access
- Anytime, anywhere
- Connecting millions
- Quicker to market
- Faster response

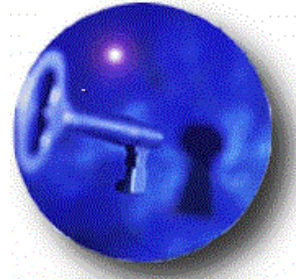




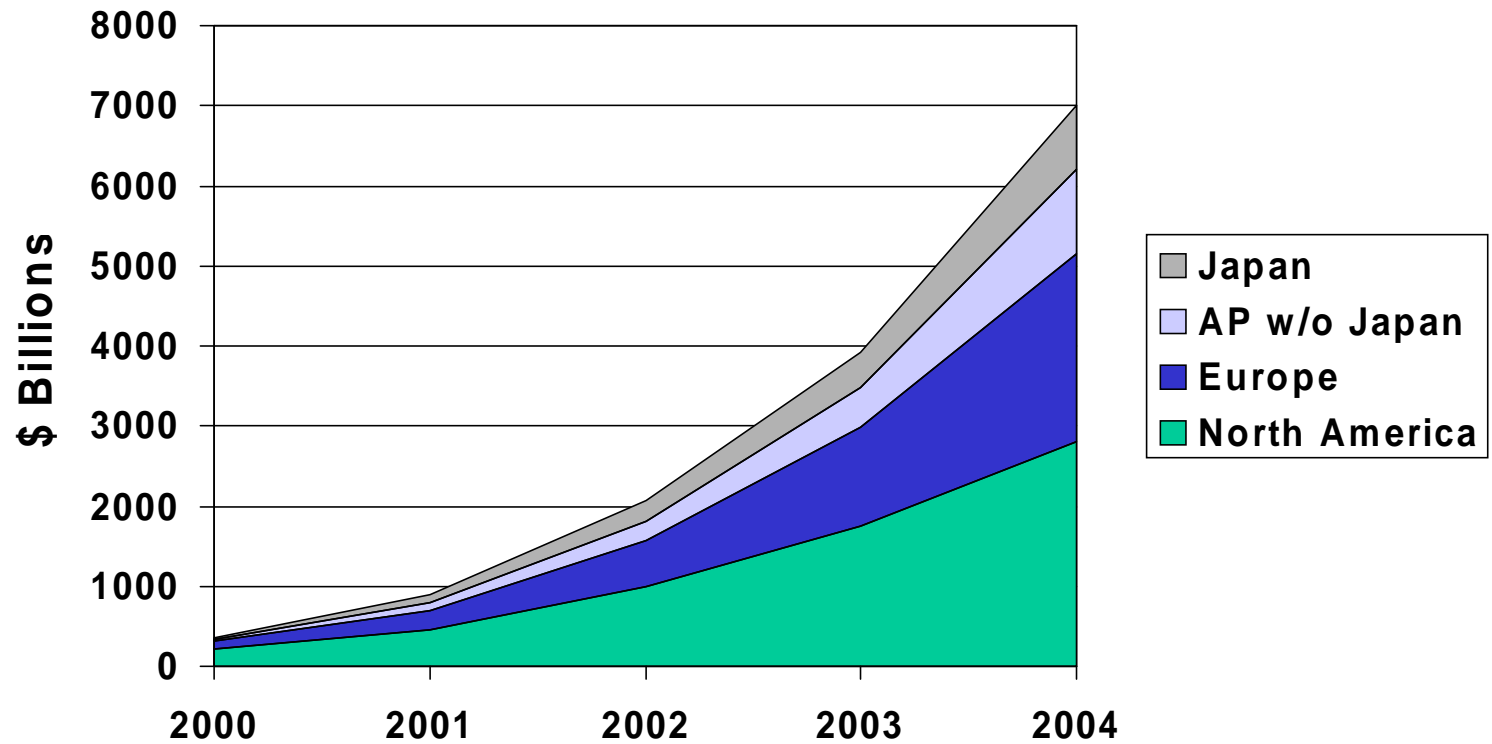
## The Explosive Growth of the Internet is Driving the Adoption of e-business



IDC 2000

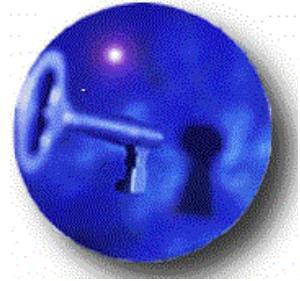


# Global B2B Trade will Reach \$7T by 2004



Gartner Group, 31.01.00





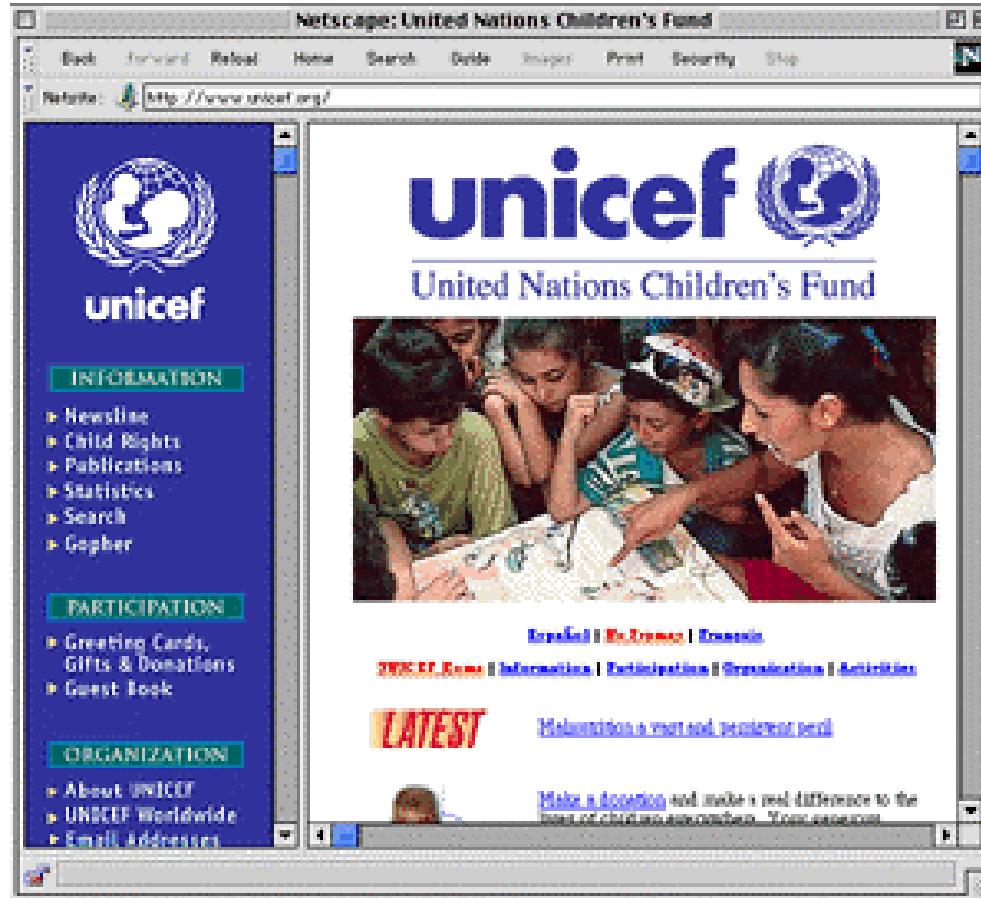
# Agenda

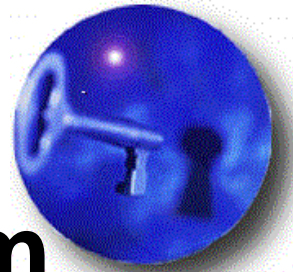
- E-business Outlook
- Internet Security Challenge
  - What are we up against?
  - What can we do about it now?
- What is the future?
  - Secure operating systems
  - Secure hardware
  - Intrusion and fraud detection



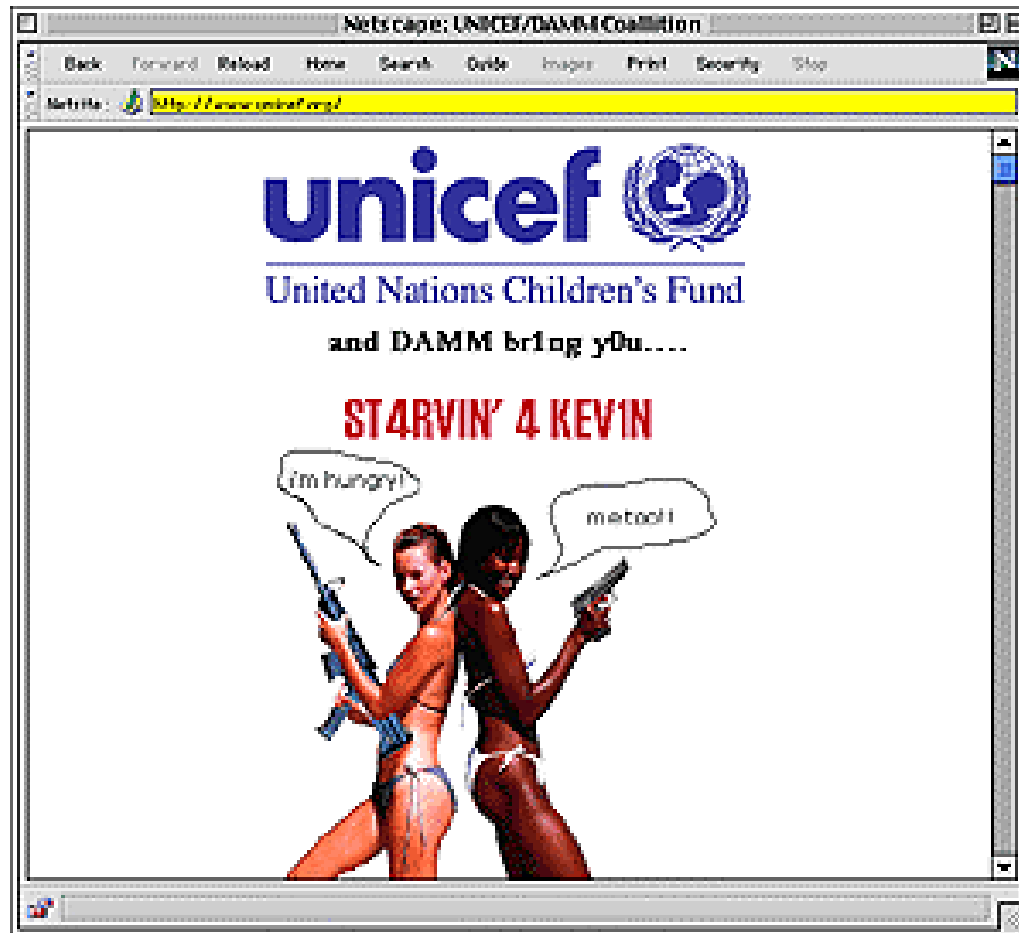


# Anyone can be a Target...





... anyone can be a Victim



ATTACK





# Why Do Hacks Happen?

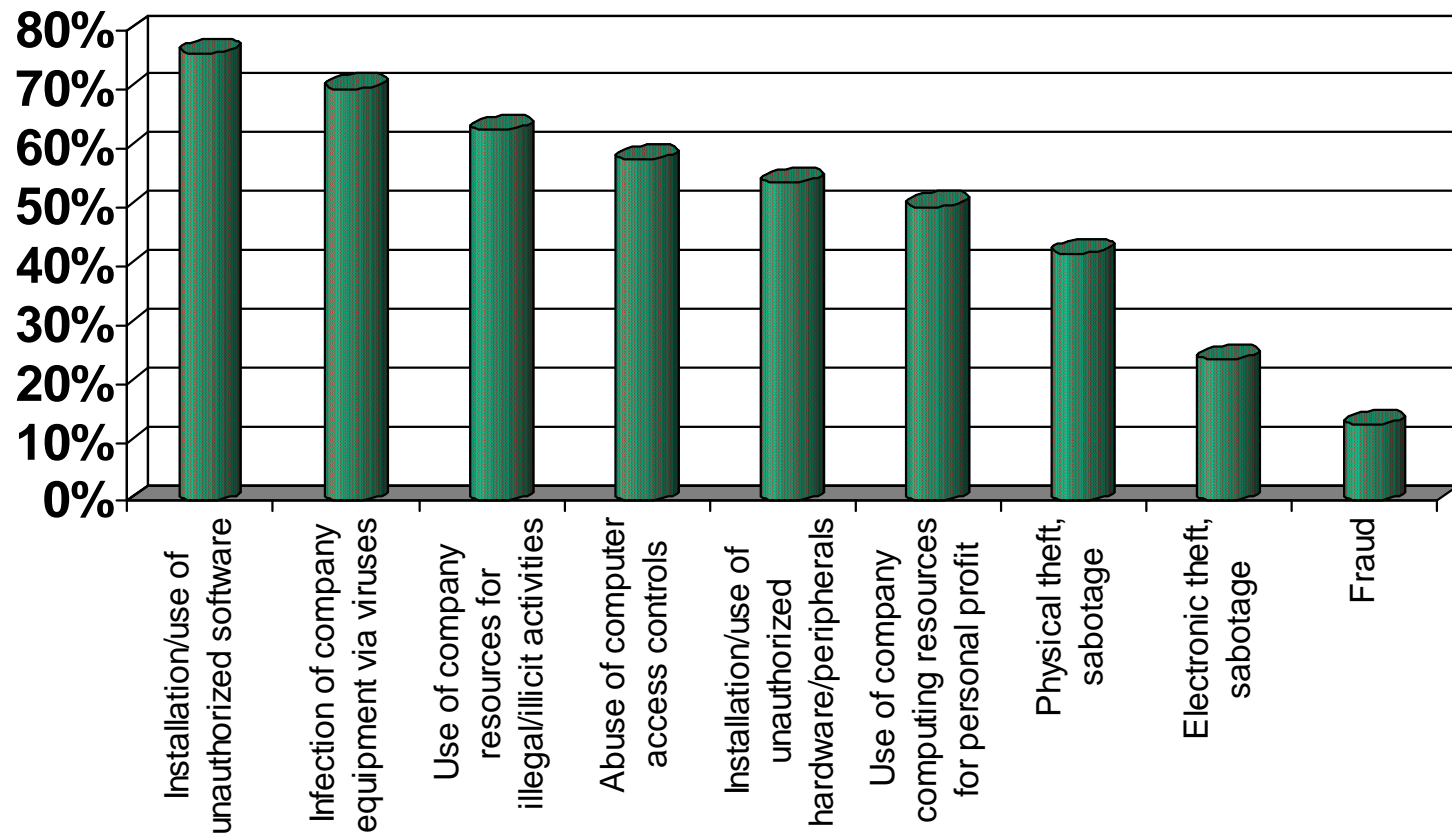
- Hacker Motivation
- Status:  
    knowledge + info + tools = ELITE HACKER!
- Sometimes socially challenged
- Willing to spend weeks to break in
- Often leave "backdoors" for later use by themselves or others





# Are the Threats Real?

## Insider Breaches



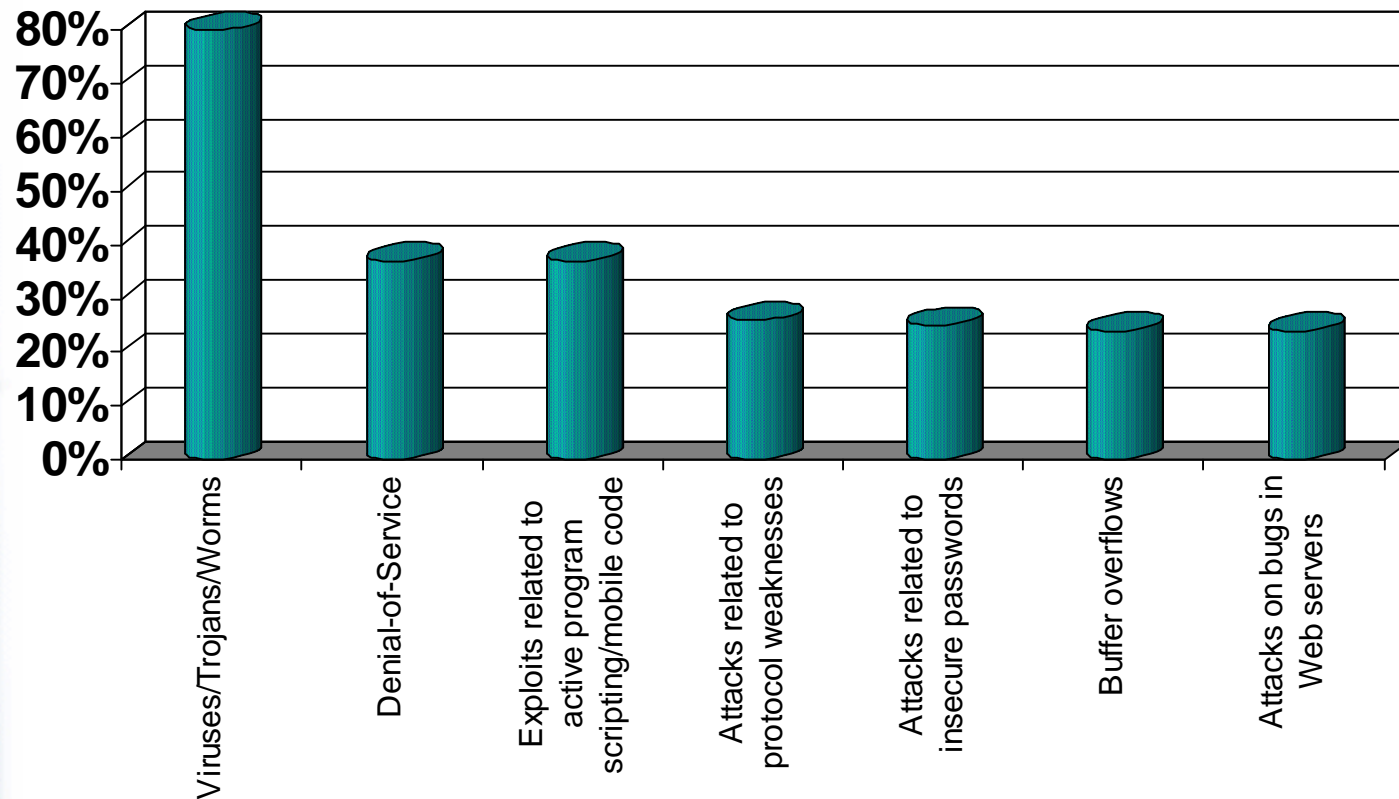
"Security Focussed", Information Security Magazine, September 2000, <http://www.infosecuritymag.com>





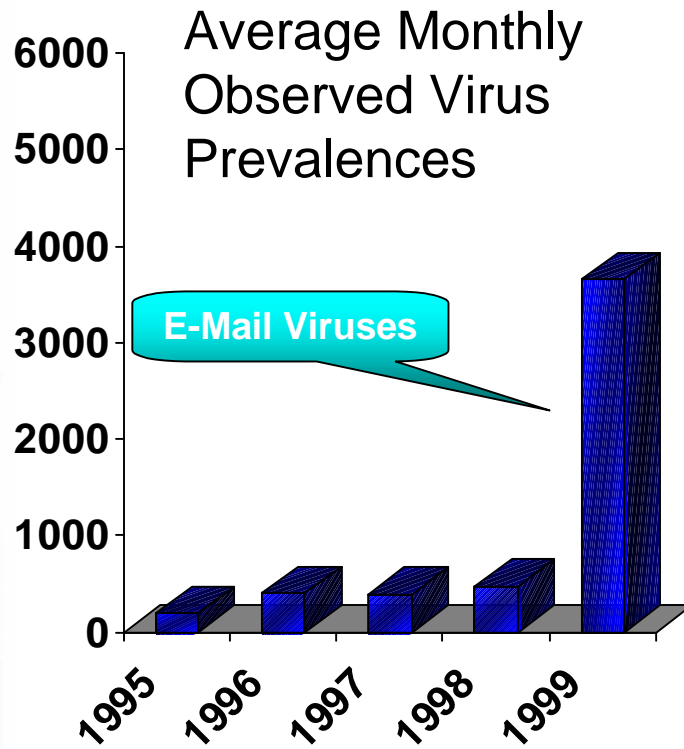
# Are the Threats Real?

## Outsider Breaches

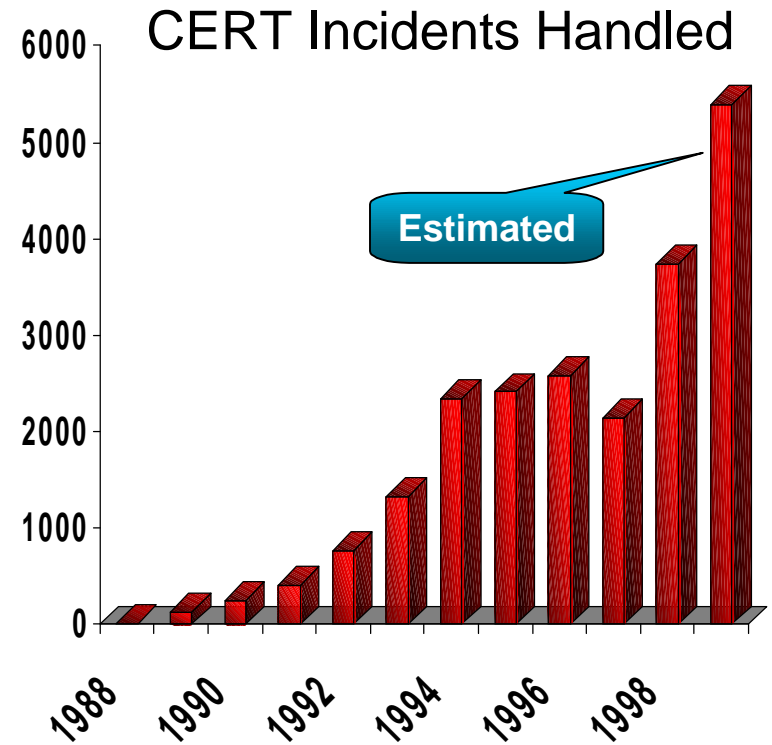




# The Threat is Real!

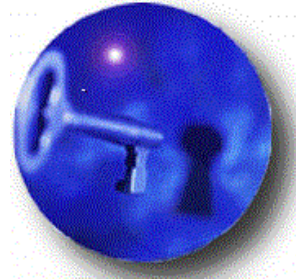


<http://www.virusbtn.com/>



[http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)

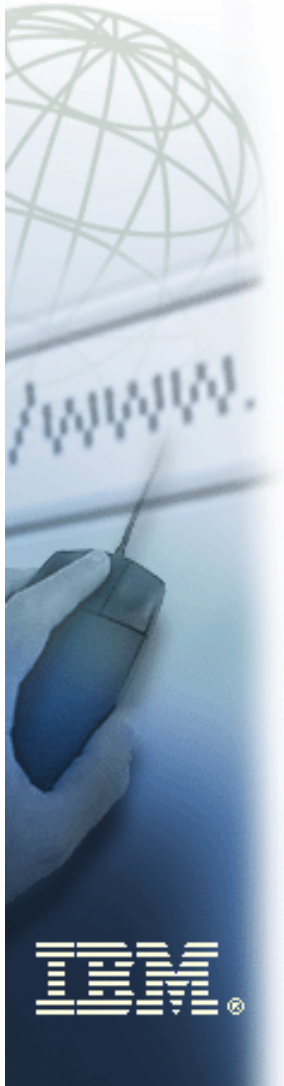




# What are the Threats?

- 2000 (1999) CSI/FBI Business Survey
- 90% (62%) reported breaches
- 74% (51%) reported financial losses,
  - 42% (31%) could quantify losses, on average \$970,000 (\$770,000)
  - stable trend: largest losses through theft of unprotected information and fraud, on average \$11M
- 25% (30%) reported outsider attacks
- 71% (55%) reported unauthorized insider access
- 27% (32%) reported Denial of service attacks

(see <http://www.gocsi.com> for more information)



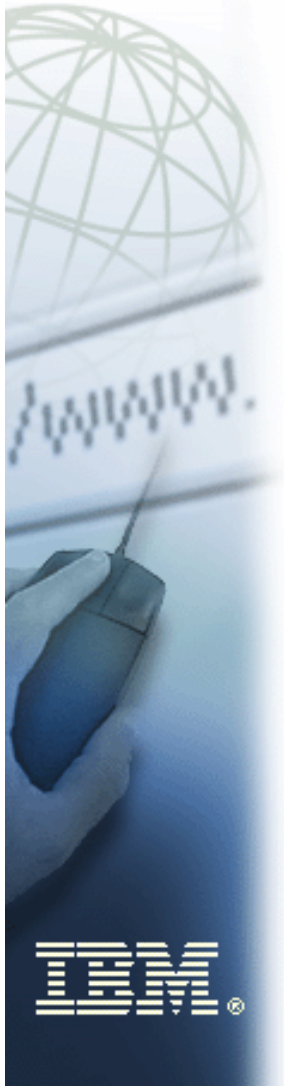


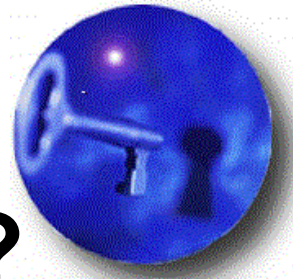
# Ethical Hacking at IBM Research

Combines Researcher's Curiosity with Business Person's Pragmatism and Urgency

Goal: "Raise the bar" for Security

- Advanced security auditing software
- Intrusion detection applications
- Secure operating system research
- Discover new "bugs" and fixes
- Executing "ethical hacks"
- Raising public awareness





# What is an Ethical Hack?

- Penetrate target's networks within the rules of engagement
- Goals:
  - (1) Can we get in?
  - (2) What can we see/do?
  - (3) Does anybody notice?
- Methods:
  - Dial-Up or Internet/Intranet/Extranet
  - Executed from IBM's highly-secured laboratory
  - Will attempt to physically enter target's site. . .
    - But only if requested

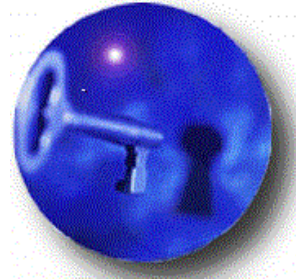




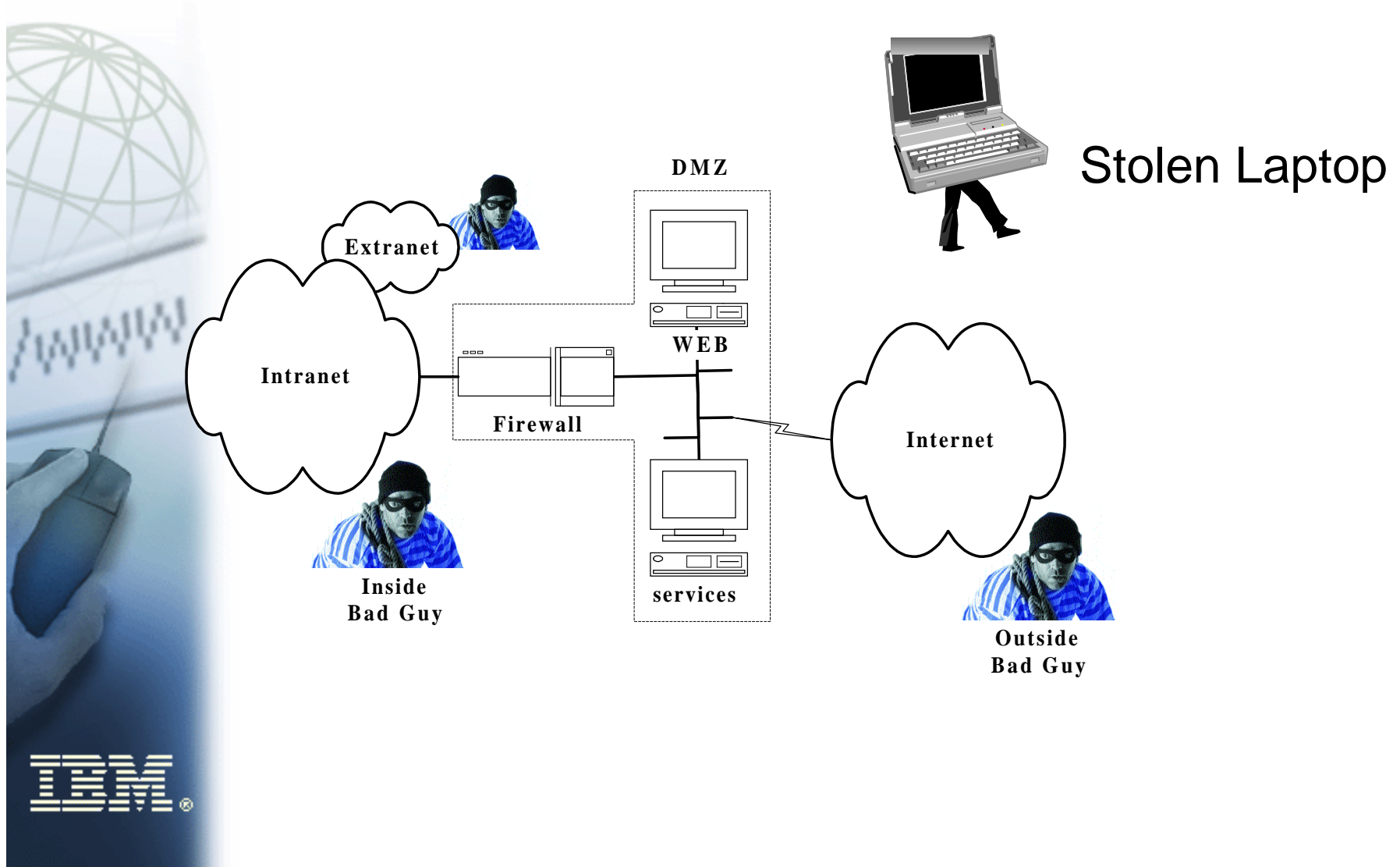
# IBM's Ethical Hackers' Win Ratio

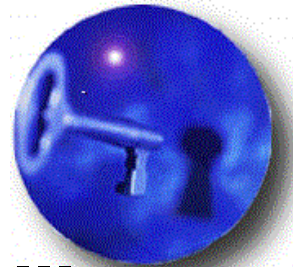
At least 80% of companies  
and organizations today  
are vulnerable to some  
kind of attack





# Hacking Scenarios





## The Top Five Vulnerabilities We See ...

- 🔓 Unsecured web servers
- 🔓 Default or weak passwords
- 🔓 Disabled access controls
- 🔓 Uninstalled security updates
- 🔓 Lack of system & network monitoring





## ... The Top Five Excuses We Hear

- "We've got a firewall"
- "My system's secure"
- "Don't have time for that stuff"
- "Security is just too expensive"
- "Hackers are just playing around ... they won't really do any real harm"





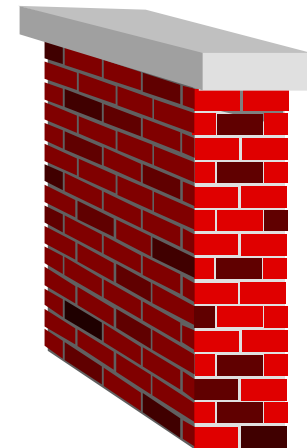
# What Can We Do About It?



Awareness  
Awareness



Technology  
Technology



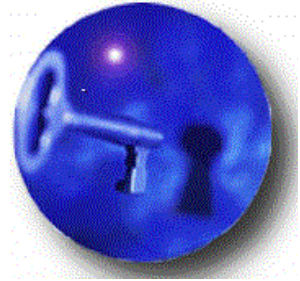


# Awareness

- Training
  - Realize that system administrators hold the keys to your company! Train them!
  - All employees need basic security training
- All employees must accept responsibility for securing their workplace

“Trust but verify”  
Random audits





# Security Policy

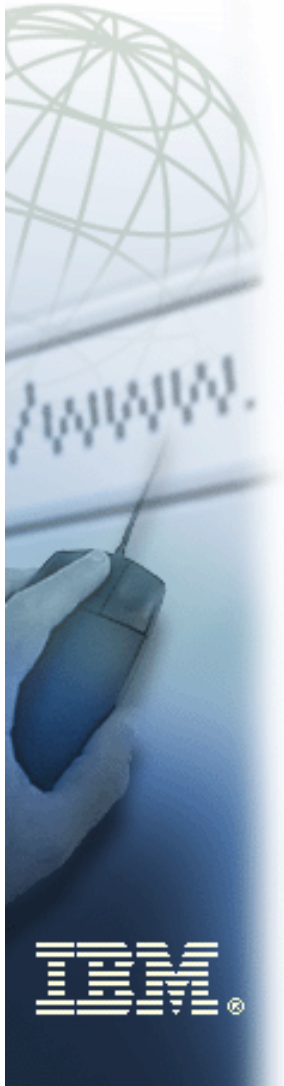
- Clearly defined, practical security policy
- Security policy should be self-enforcing
- Corporate systems should be "secure by default"
- External and internal network connectivity must be controlled and monitored





# Security Policy Includes a Privacy Policy

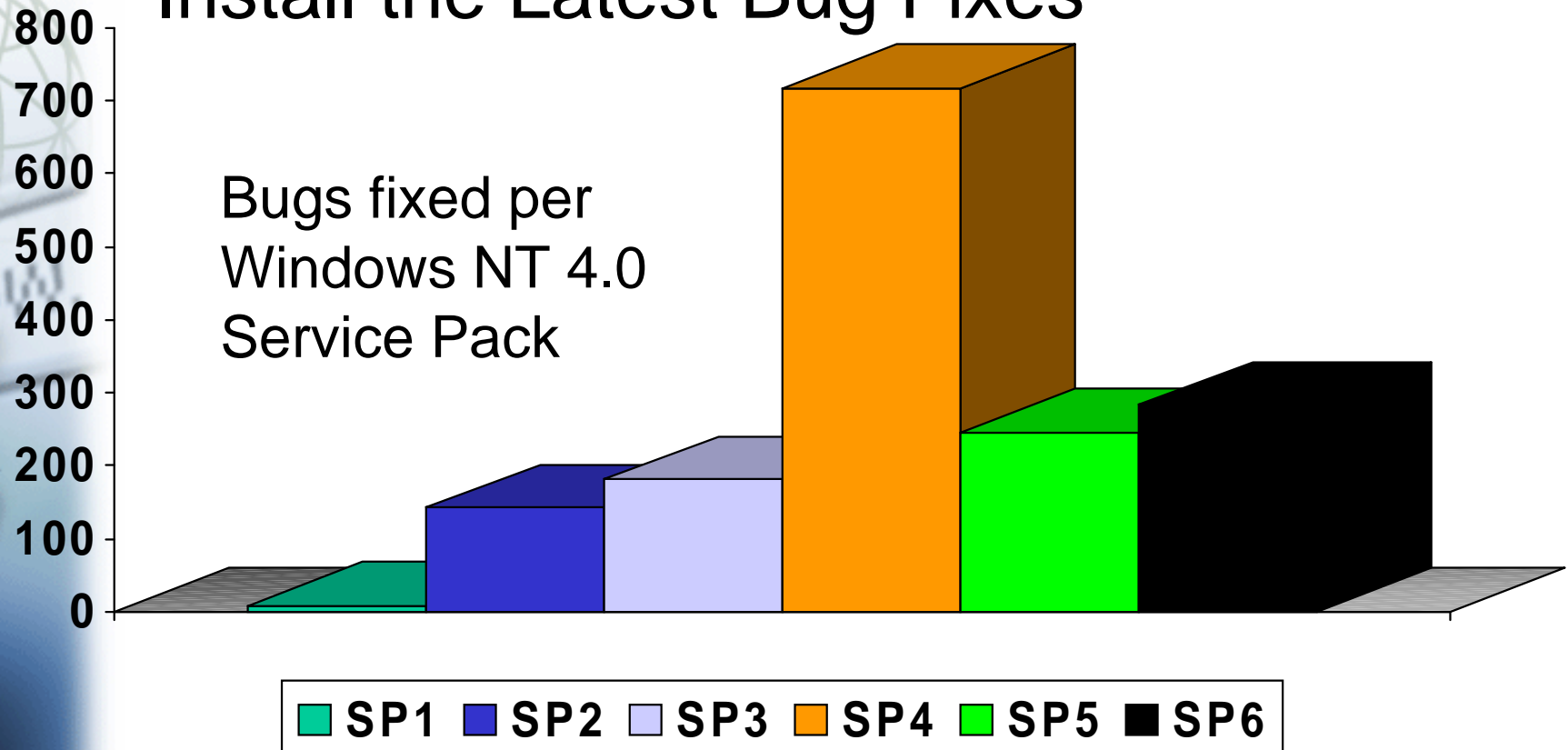
- Consumer concern over privacy is a potential inhibitor to the growth of the Internet
- All public and private web presence should have a link to a privacy policy statement
- Only gather and maintain online information that you really need online
- Internal access to private information can be just as damaging!





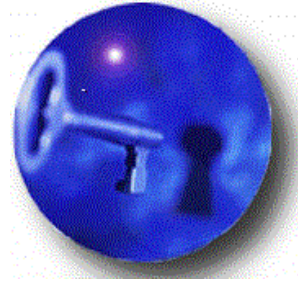
# Security Technology

## Install the Latest Bug Fixes



<http://support.microsoft.com/support/>





# Security Technology

- Regular auditing
  - Automatic and manual
- Real-time intrusion detection
  - Network and system based
- Anti-virus software
- Firewalls
- Virtual private networks (VPNs)

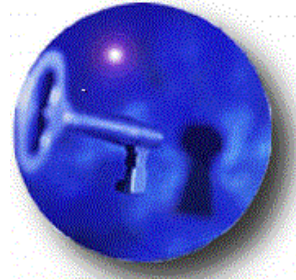




# Agenda

- E-business Outlook
- Internet Security Challenge
  - What are we up against?
  - What can we do about it now?
- What is the future?
  - Secure hardware
  - Secure operating systems
  - Intrusion and fraud detection





# Strong Encryption

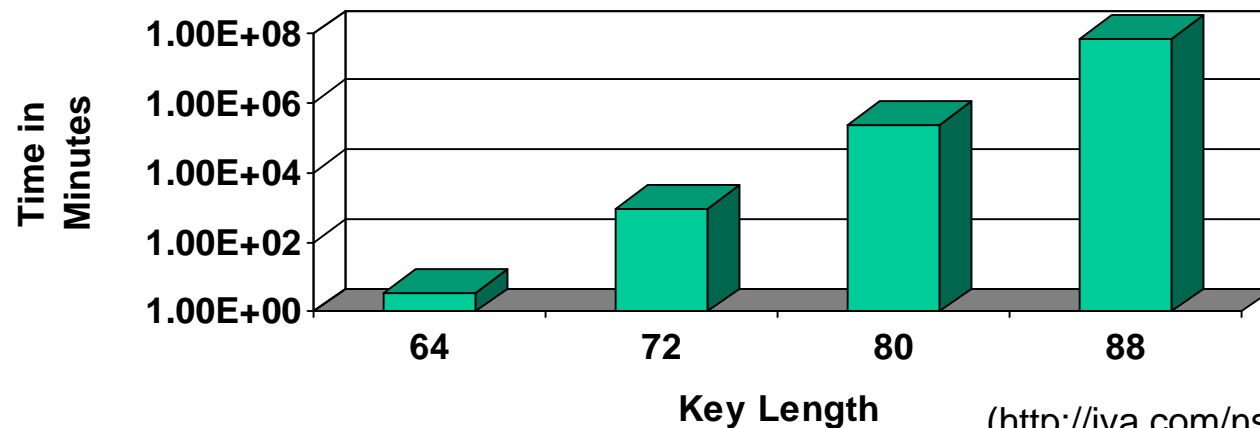
## Fact

- Cryptographic operations workload increases **linearly** with key length
- Brute force analysis workload increases **exponentially** with key length

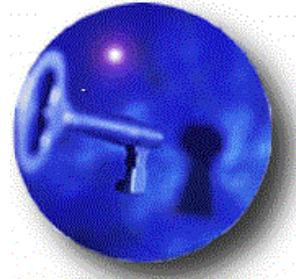
## State of the Art in 1999

- 56-bit DES cracked in 56 hours by EFF engine [Crypto98]
- RSA155 (~512-bit) number factored in less than 6 months [RSA99]

## Possible NSA Decryption Capabilities



(<http://jya.com/nsa-study.htm>)



# Future Technologies

🔒 Cryptography secures the network

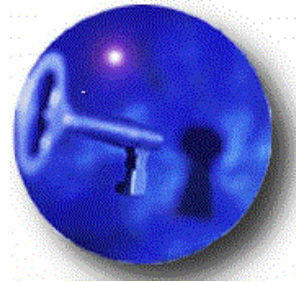
🔓 Attackers will go the way of least resistance:

- ▶ Client systems and applications
- ▶ Server systems and applications

→ Secure at least the valuable information such as the cryptographic keys

→ Find out when somebody breaks in





# Securing Valuables

- Tamper-resistant and -responding hardware
  - Smart Cards
  - Coprocessors (e.g., IBM 4758)
- Evaluated and certified software





# Tamper-Resistant and Responding Hardware



IBM 4758 PCI  
Cryptographic Coprocessor



FIPS 140-1 Level 4 certified

- Evaluator may use all imaginable attacks
- Software and hardware underwent formal modeling to prove the security properties





# Aren't These Just Bugs?

- Can we just find and fix them? Will the software get stable over time?
- Yes - they are just bugs.
- No - the software won't just stabilize over time
- Our current research shows that:
  - Hundreds of new vulnerabilities found per year
  - None of the software is getting stable
  - The same classes of bugs are being found over and over again in both new and old software
- Why?
  - Sheer complexity of most software
  - Lack of security concern and knowledge by most developers
  - Push for new features
  - Push for shipping software without time for design or review or good coding practices or testing or documentation





# Linux Security Problem

- Authentication
  - Kernel abdicates responsibility via `setuid()`
    - Trusted Computing Base (TCB) is unbounded in size.
    - Provides weak or no authentication
  - Violates principle of least privilege
- Authorization
  - No Mandatory Access Control





# Skeptix - Secure Linux

- Goal: significantly improve Linux resistance to attack
- Eliminate `setuid()` and root account
- Add fine-grained per-process privileges
  - Processes can only give up privileges
- Strong authentication is the only way to gain privileges
  - interactive: challenge-response
  - automatic: via digital signatures





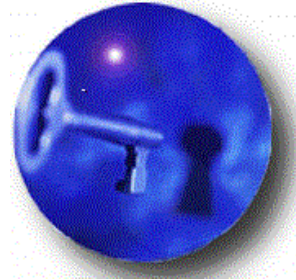
# Skeptix - Secure Linux

- Minimize performance impact (<5%)
- Application sandboxes (includes attack containment)
  - non-executable stack (Solar Designer)
- IPSEC
- Encrypting file system
- Secure deletion as fs mount default
- per authenticated session /tmp





# Intrusion (and Fraud) Detection

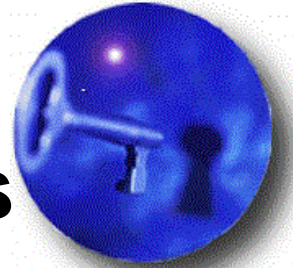


- Find out when somebody breaks into the
  - network
  - servers
  - applications
- Help security administrator with recommended actions to:
  - determine the kind of attack
  - trace back the attacker
  - respond to the attack

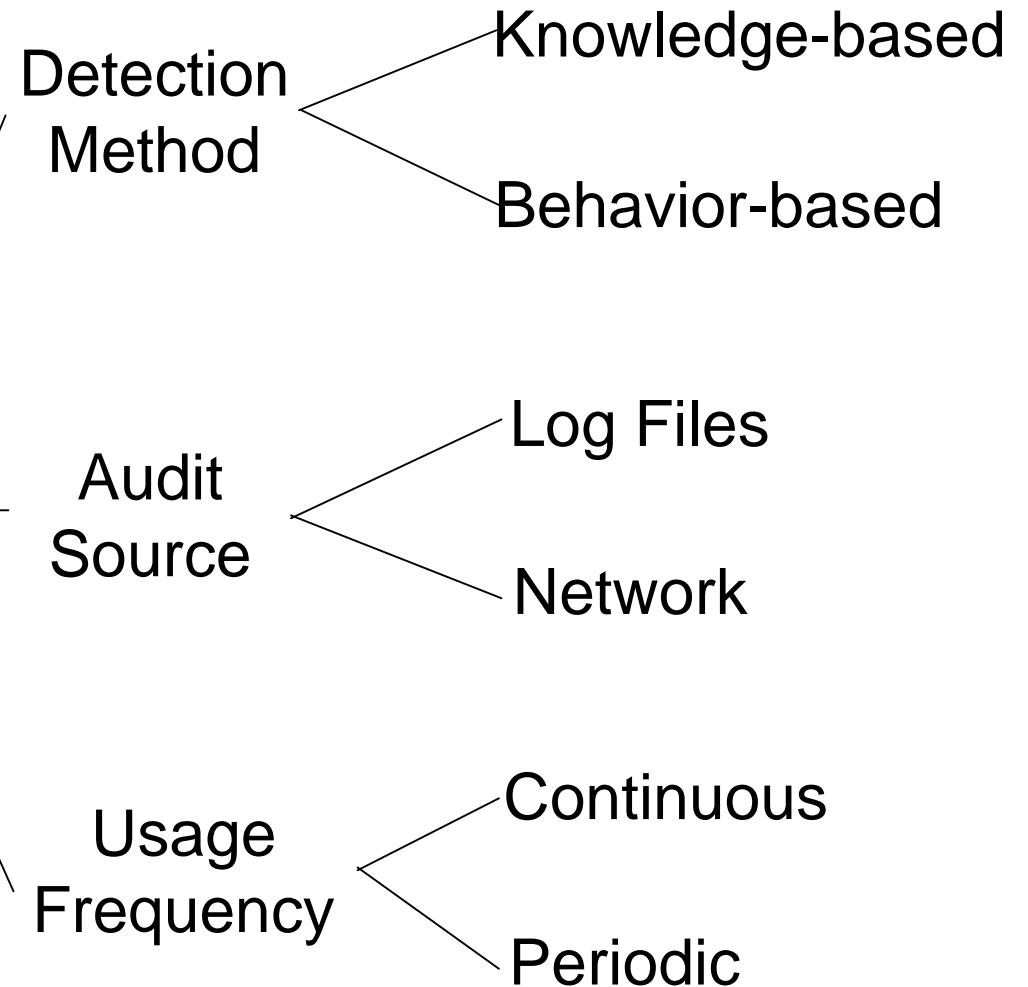




# Intrusion Detection Techniques



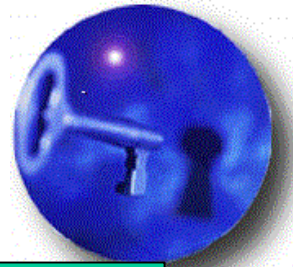
Intrusion Detection  
Sensors





e-business

# Web Intrusion Detection System

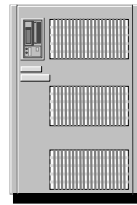


Signatures of known attacks

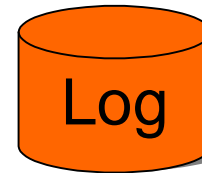
Attacker sends hostile HTTP-requests



Web Server

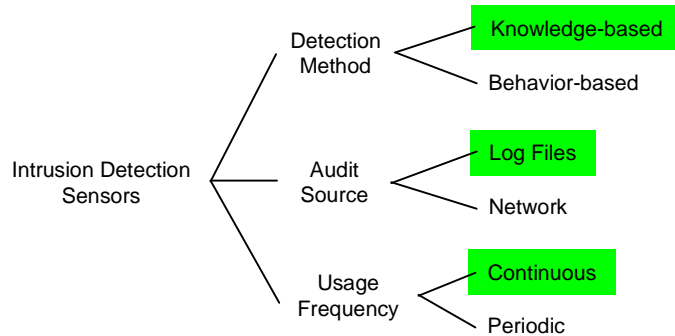


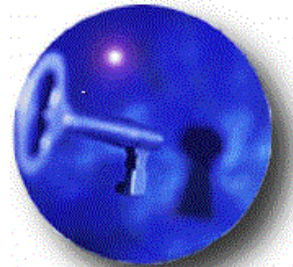
Entry for every request



Web IDS

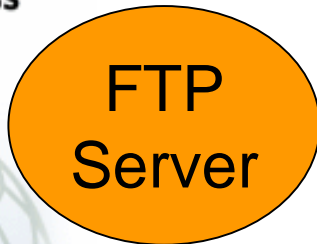
Alarm



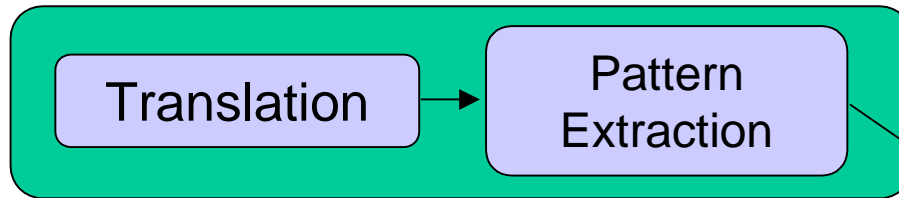


# Demon Watcher

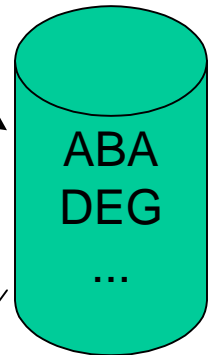
Training Phase



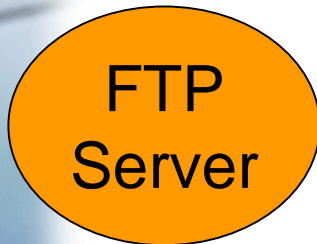
PROC\_create  
FILE\_open  
FILE\_close  
...



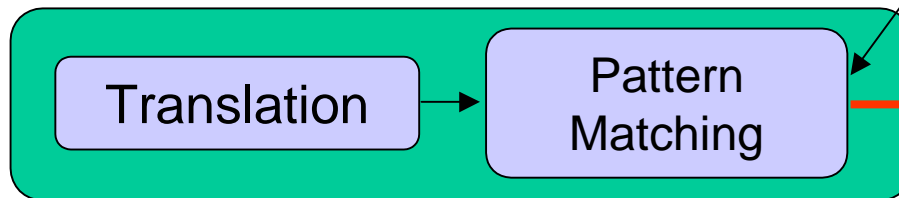
...ABADEABA...



Production Phase

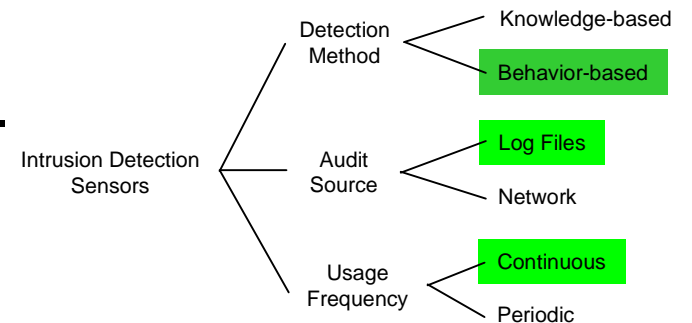


PROC\_create  
FILE\_open  
PROC\_create  
FILE\_close

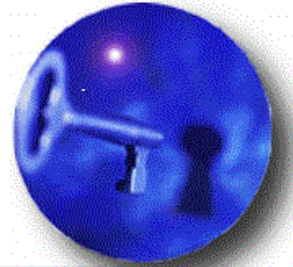


...ABADE**E**BABA...

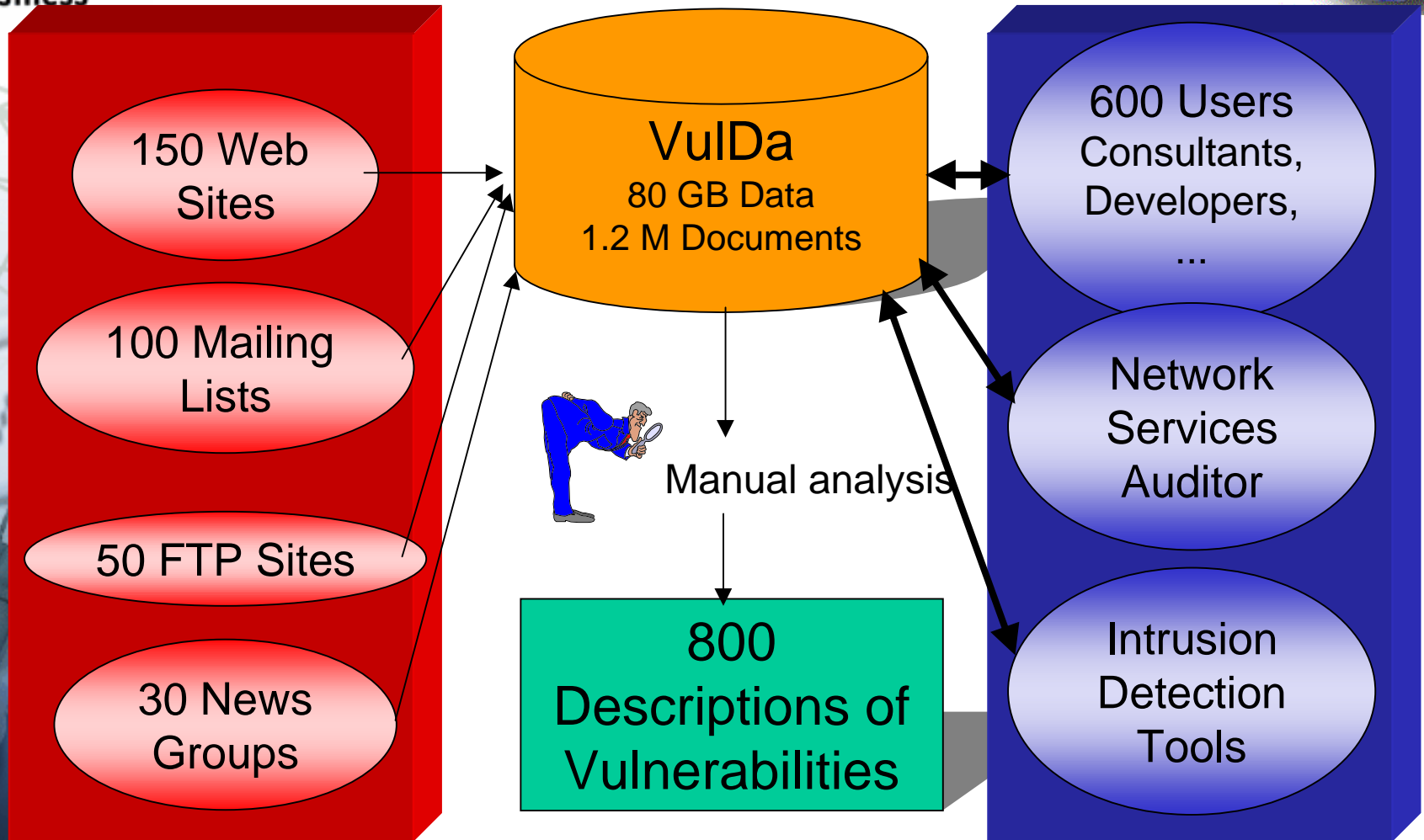
Alarm



# @VuIDa - The Vulnerability Database



e-business



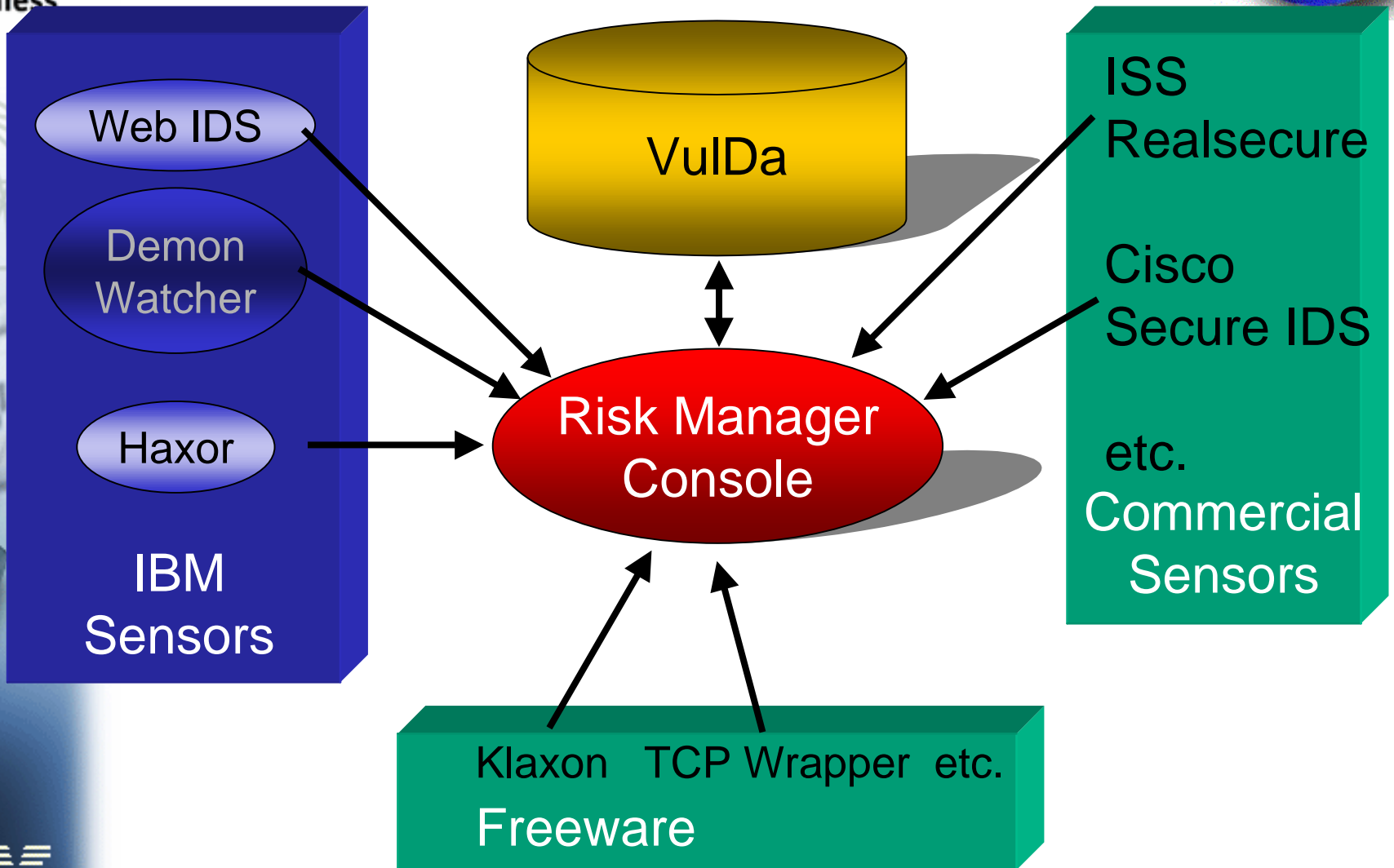
Internet

IBM Intranet

# Tivoli SecureWay Risk Manager



e-business



# Tivoli SecureWay Risk Manager



**Tivoli SecureWay Risk Manager [Event View]**

File View Tools Windows Help

**Top 10 hosts**

**Top 10 event classes**

**Top 10 administrators**

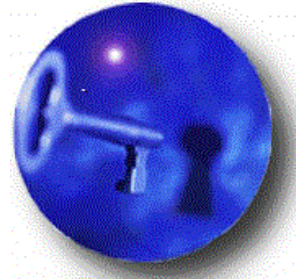
**Actionable Events**

date_reception	class	hostna...	status	severity	msg
06-Aug-98 4:26:27 PM GMT	TEC_Start	sunnik	RESPONSE	CRITICAL	message56
06-Aug-98 4:35:59 PM GMT	Root_Login...	mbaldass	ACK	CRITICAL	message46
06-Aug-98 5:34:36 PM GMT	No_Memory	ncafaro	OPEN	FATAL	message85
06-Aug-98 8:40:13 PM GMT	TEC_Error	mbaldass	OPEN	CRITICAL	message50
06-Aug-98 10:15:28 PM GMT	TEC_Error	jmills	RESPONSE	CRITICAL	message95
06-Aug-98 10:17:38 PM GMT	TEC_Stop	jmills	ACK	FATAL	message59
06-Aug-98 11:07:48 PM GMT	TEC_Error	jmills	ACK	CRITICAL	message14

Ack Close Reopen Help

**Incoming Events**

date_reception	class	hostname	status	severity	msg
10-Nov-98 6:42:4...	TEC_Start	jmills	OPEN	HARMLESS	TEC Event Serv...
07-Aug-98 6:24:5...	TEC_Error	sunnik	ACK	CRITICAL	message3
07-Aug-98 1:46:4...	No_Proc_Slots	pdeidda	OPEN	FATAL	message73
07-Aug-98 4:08:2...	TEC_Start	mbaldass	RESPONSE	FATAL	message73
07-Aug-98 3:31:3...	Server_OK	jmills	OPEN	MINOR	message47
07-Aug-98 2:30:0...	No_Memory	jmills	OPEN	HARMLESS	message76
07-Aug-98 1:00:0...	TEC_Stop	sromanel	OPEN	UNKNOWN	message0
06-Aug-98 7:56:4...	No_Memory	pdeidda	OPEN	CRITICAL	message17
07-Aug-98 9:36:3...	No_Memory	sunnik	ACK	FATAL	message80
07-Aug-98 10:26:...	TEC_Start	ncafaro	ACK	WARNING	message31
07-Aug-98 12:17:...	TEC_Stop	sunnik	RESPONSE	MINOR	message33
06-Aug-98 7:02:4...	TEC_Error	ncafaro	ACK	MINOR	message51



# Summary

- e-business is rapidly taking off
- This growth has also caused a growth of security incidents
- We need to focus on Awareness, Policy, and the right security Technology to cope with these incidents
- The end-points are the weakest links in the security chain
- Formally evaluated and certified secure software and hardware will be the means of choice to safeguard the electronic valuables of the information society
- Intrusion and fraud detection become increasingly important to deal with the vulnerabilities of existing software solutions

