Introdução ao
Segurança do computador

Vítor Francisco Fonte
vff @di .uminho.pt

2019/20

Curso de Mestrado em Engenharia Informática

Universidade do Minho

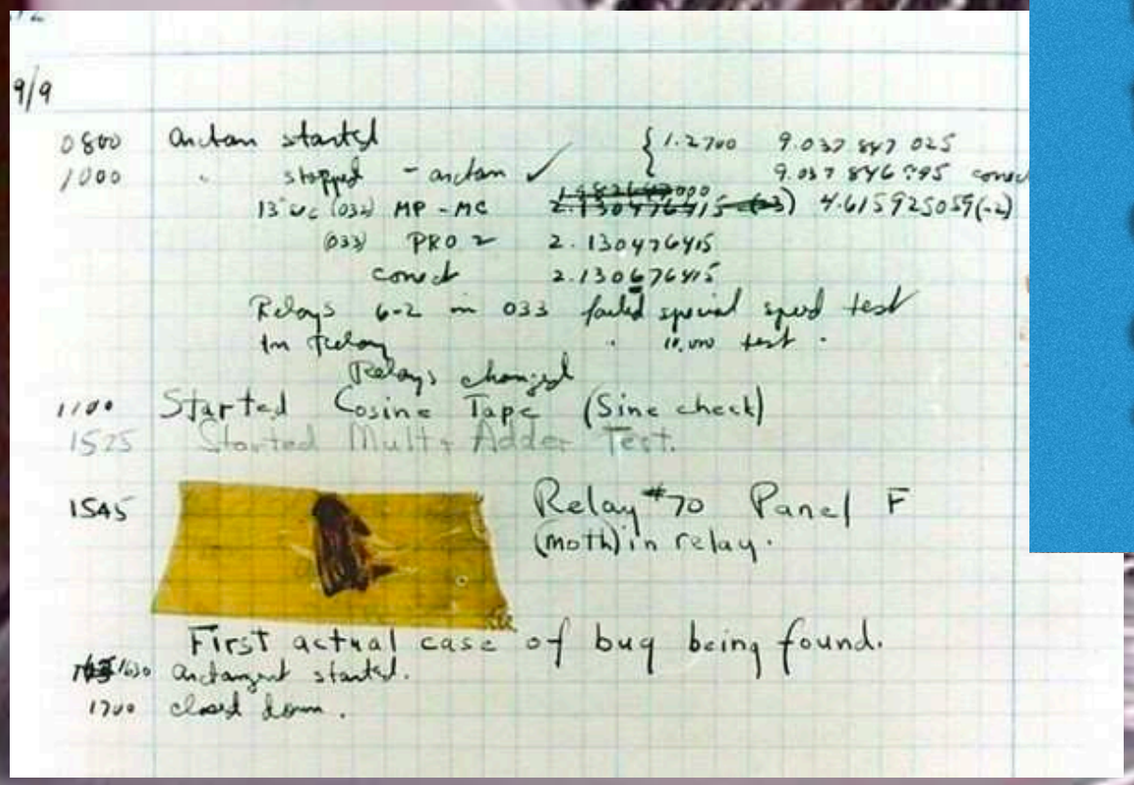
Introdução

- O que é “segurança”?
  - di ff erent coisas para di ff erent pessoas
- Foco original versus atual da segurança do computador:
  - sistemas multiusuário versus distribuídos usuários não confiáveis versus dispositivos de rede não confiáveis manter os usuários separados versus
  - proteger os ativos acessíveis à rede
  -
- Ataques e atacantes:
  - diferentes atores, objetivos e motivações
  - diferentes métodos e níveis de especialização

Um pouco de história

1945

Primeiro “bug”. Grace Murray Hopper grava um ser mariposa encontrado preso entre o relé contatos de Harvard Mark II computador. Daí os termos “bug” e “depuração”.



Um pouco de história

1964

A era “phreaking”. AT&T inicia Vigilância de fraude de portagem “Greenstar” sistema, monitorando chamadas de longa distância feita a partir de telefones públicos tentando pegar “aberrações telefônicas” (ou “phreakers”), pessoas que fazem chamadas gratuitas usando “azul caixas”. Estes eram dispositivos simples reprodução de tons de controle da AT&T.

Um pouco de história

A bit of history

1972

Freaking de cereais. John Drapper descobre que ele poderia fazer livre chamadas na rede telefônica AT&T usando simplesmente o apito oferecido dentro de cereais Cap'n Crunch caixas. O apito produz um 2600Hz som... exatamente o que é necessário para desbloquear a rede AT&T.

Cereal phreaking. John Drapper discovers that he could make free calls on the AT&T telephone network simply using the whistle offered inside Cap'n Crunch cereal boxes. The whistle produces a 2600Hz sound... exactly what it takes to unlock the AT&T network.

Um pouco de história

1979

O primeiro “verme”. Em Palo Alto Xerox Centro de Investigação, John F. Schoch e Jon A. Hupp começar a desenvolver programas de auto-reprodução infectando os computadores Alto conectados ao mesma rede. Estes “vermes” são volátil, seu propósito é benigno (pesquisa do sistema distribuído), e sancionada pela organização Xerox.

Um pouco de história

1986

O primeiro “vírus”. Irmãos paquistaneses Basit e Amjad Farooq Alvi desenvolvem o “O Cérebro”, o primeiro pessoal programa de computador que propaga através da infecção do setor de inicialização de dispositivos de armazenamento. A infecção não destrói dados do usuário e ele ainda fornece o contato informações de seus autores.

Um pouco de história

A bit of history

1986

Primeiro trabalho ARPANET. Robert Morri desenvolve o primeiro trabalho de computador que propaga através de ARPANET (antecessor da Internet). O verme replica e preenche toda a memória disponível sobre o (mais de seis mil) infectados computadores, tornando-os inoperacional. Acusado por 3 anos de prisão suspensa sentença e uma multa de 10.000 USD.

Um pouco de história

A bit of history

1990

Primeiro vírus automodificável. O vírus muda com cada renderização de replicação código tradicional ineficaz baseado em assinatura detecção.

1995

O primeiro vírus explorando o Microsoft Word. O vírus “Conceito” infecta sistemas em abertura de documentos do MS Word (via macros).

Um pouco de história

A bit of history

1998

Controle remoto de sistemas militares e civis. Dois adolescentes dos EUA conceber e executar operação “Solar Sunrise” terminando controlando mais de 500 infraestruturas informáticas militares e civis.

2000

Negação de Serviço Distribuída. Computadores da Universidade da Califórnia são usados para inundar redes informáticas e tornar inoperacional sites como Amazon, Yahoo, eBay,...

2001

“Código Vermelho”: 2 bilhões de dólares em danos. O termo tenta infectar sistemas MS Windows NT e 2000, com o objetivo final de um ataque distribuído à Casa Branca Infra-estrutura de TI. O worm é decifrado apenas a tempo de Impedir o ataque.

Um pouco de história

2005

“PoinsonIvy”: vírus e controle remoto em um único pacote. Os sistemas infectados são controlados pelo malware (um remotamente acessível “backdoor” também está disponível para o Ele pode atividade do sistema de gravação, ativar a câmera de vídeo e microfone (se disponível). Ele baixa e executa “payloads” disponibilizados a partir do sistema remoto de ataque. Foi. desenvolvido a fim de roubar segredos da defesa e indústria química.

2006

“Nyxem.e”: o limpador de arquivos. Este worm limpou MS Documentos do Office e Adobe (entre outros aplicativos) dos sistemas de arquivos infectados, no terceiro dia de a cada mês. Centenas de usuários foram afetados.

Um pouco de história

2008

“Koobface”: difunde-se através de e-mail e redes sociais. Ele exibe falso anúncios (ex. no Facebook) de produtos que uma vez comprados nunca são entregues à vítima.

2010

“Stuxnet”: ataque a sistemas de controle industrial. Extremamente malware complexo que atacou sistemas SCADA específicos. Sua principal vítima foi a infra-estrutura de enriquecimento nuclear iraniano. Agências de inteligência dos EUA e israelenses são suspeitos de ter esteve envolvido em seu desenvolvimento e implantação.

2012

“Heartbeat”: um mas em OpenSSL. Esta vulnerabilidade foi detectado na biblioteca criptográfica OpenSSL, e permite o acesso a comunicações cifradas e armazenadas dados. Milhões de sistemas e bilhões de usuários foram afetados.

Um pouco de história

2013

Roubo de dados pessoais de mais de 70 milhões usuários. Baseado nos EUA Relatórios de negócios de varejo de destino que uma grande parte de seus clientes tinham seus dados pessoais registros roubados do computador da empresa sistemas.

2014

Roubo de 1,2 bilhão de criativos de autenticação. russo hackers exploram (através de um vírus de computador) vulnerabilidades no manipulação de instruções SQL em vários sites e foram capazes de coletar as credenciais de autenticação de seus usuários. Mais de 500 milhões de contas de e-mail também podem ter sido comprometidas.

Estónia, 2007

- Um ataque cibernético dirigido a um país:
  - Negação de Serviço Distribuída: “ping inundação” usando “botnets” alugados
  - controle de vários sites (especialmente na mídia): injeção de comentários (spam) e substituição de conteúdo (defacement)
- Sítios Web de diferentes instituições:
  - parlamento nacional, ministérios, meios de comunicação social, instituições financeiras,...
- Considerações
  - nunca antes visto coordenação e âmbito
  - guerra cibernética ou ciberterrorismo?

Estónia, 2007

- Considerações
  - algumas semelhanças com a operação Titan Rain (2003-06) e ao ataque
  - algumas semelhanças com os ataques ocorridos na Ossétia do Sul (2008)
  - segurança de rede acaba sendo integrada na doutrina militar moderna
- Estónia implanta “embaixadas digitais” em países amigáveis
  - mitigar riscos e ameaças à sua infraestrutura
  - redundância melhorada: disponibilidade e integridade dos dados
  - continuidade de negócios: governo, administrador público. e prestação de serviços

Stuxnet, 2012

- Alvo:
  - sistemas de controle industrial SCADA muito específicos
  - principalmente um ff ecting o programa de enriquecimento nuclear
  - iraniano

- Atacantes:
  - Agências de inteligência dos EUA e israelenses suspeitas de estar por trás deste ataque

- Divulgação e eliminação:
  - Infecção inicial através de unidades flash USB, primeiro avistado na natureza em 2010 Em
  - seguida, infectar computadores em redes privadas não conectadas à Internet Definido para
  - parar e excluir a si mesmo em 24 de janeiro de 2012
  -

Stuxnet, 2012

- Segmentação por ataque em camadas:
  - Sistemas operacionais Microsoft Windows executando...
  - Siemens PCS 7, WinCC e STEP7 aplicações industriais, rodando...
  - em um ou mais PLCs S7 da Siemens.
- Exploiting multiple vulnerabilities:
  - 4 anteriormente desconhecido (0 dias), extremamente raro
  - 2 já desconhecido

Stuxnet, 2012

- Desafio técnico:
  - ataque muito complexo
  - combinando di ff erent tipos de malware
  - várias linguagens de programação
  - componentes de software de nível de usuário e kernel (rootkit)
  - drivers (kernel) digitais assinados com
  - chaves digitais também roubadas de duas empresas sediadas em Taiwan

Snowden: NSA, 2013

- Ex-funcionário da CIA, NSA, Dell e Booz Allen Hamilton
  - especialista em segurança de redes e ciber-contramedidas
- Divulgação não autorizada de documentos revelando segredos Acordos entre agências internacionais de informação:
  - NSA e outras agências de informação dos EUA Austrália (ASD), Reino Unido
  - (GCHQ), Canadá (CSEC), Dinamarca (PET), França (DGSE), Alemanha (BND), Itália (AISE), Países Baixos (AIVD), Noruega (NIS), Espanha (CNI), Suíça (NDB), Singapura (SID) e Israel (ISNU)

Snowden: NSA, 2013

- Sistema de vigilância global
  - combinando várias agências, ferramentas e técnicas coleta não direcionada de dados de várias fontes (Dragnet) compartilhamento de dados brutos para
  - mineração em tempo real ou posterior
  -

- Principais revelações:
  - ordem judicial secreta concede à NSA acesso a registros telefônicos de cidadãos
  - dos EUA PRISM permite o acesso direto aos serviços de empresas tecnológicas americanas, como Google, Facebook, Microsoft e Apple GCHQ (Reino Unido)
  - conecta redes de fibra óptica em todo o mundo NSA espião em países estrangeiros
  - e líderes mundiais

Snowden: NSA, 2013

- Principais revelações (continuação):
  - o programa Xkeyscore pode procurar quase tudo o que um usuário acessa e publica na Internet a Operação de Acesso Personalizado (TAO) é uma equipa
  - especializada em comprometendo a segurança em sistemas remotos, infectando-os com malware a NSA tenta quebrar protocolos criptográficos e
  - minar a Internet Segurança

  - a NSA pode interceptar conexões com os dados do Yahoo e do Google centros a NSA intercepta o Serviço de Mensagens Curtas (SMS) a NSA
  - intercepta chamadas telefônicas nas Bahamas e no Afeganistão
  -

Eleições Presidenciais dos EUA, 2016

- Instrumentação de redes sociais
  - manipulação de redes sociais como Twitter e Facebook criação automatizada ou manual de contas de usuário em grande escala postagem e compartilhamento
  - automatizados de conteúdo falso ou enganoso compartilhamento automatizado de conteúdo para aumentar sua visibilidade (tendências) conteúdo de tendência
  - tendem a ser automaticamente sugerido para usuários reais ataque muito eficaz capaz de disseminar ideias pretendidas
  -
  -
  -
- O ataque do Comitê Nacional Democrático (DNC)
  - acesso não autorizado aos servidores de e-mail DNC vazamento de e-mails sensíveis para a mídia através do Wikileaks
  -

Wikileaks: CIA #Vault7, 2017

- Ferramentas para comprometer a segurança de smartphones (iOS e Android), computadores pessoais (Windows e OS X) e até mesmo carros, a fim de explorá-los como dispositivos de monitoramento, audição e geo-tracking

- Há uma base secreta em Frankfurt, Alemanha, responsável por ciber-operações de espionagem na Europa, Oriente Médio e África

- O programa Weeping Angel pode explorar Smart TVs Samsung e usar -los como dispositivos de escuta, mesmo em espera

- Um malware foi desenvolvido para mascarar a origem/autoria de ataques, plantar evidências falsas do envolvimento de entidades estrangeiras

- Menos de 1% dos documentos deste tesouro foram revelados ao público

Eleições Francesas, 2017

- Mais de 9 GB de e-mails e outros documentos foram roubados dos servidores de campanha de Emmanuel Macron
- Os documentos foram vazados em um site russo de compartilhamento de arquivos
- Evidência de tentativas de eliminar metadados deixados para trás
- APT 28 é suspeito de estar por trás desses ataques
  - APT significa ameaça persistente avançada APT 28 acredita-se estar ligado
  - à inteligência russa APT 28 também é suspeito de estar envolvido nos EUA
  - 2016 Ataques de eleições presidenciais

Modelo de ameaça

- Quais são os bens que queremos proteger?
  - Qual é o valor deles?
- Quem são os atacantes, motivações e capacidades?
  - O que podemos esperar que eles tentem?

Modelo típico de ameaça

- O atacante é o mais forte possível
- Mas não é possível quebrar criptografia (e possui a rede)

- Embora:
  - a maioria dos atacantes são mais fracos do que este
  - criptografia incorreta pode ser quebrada

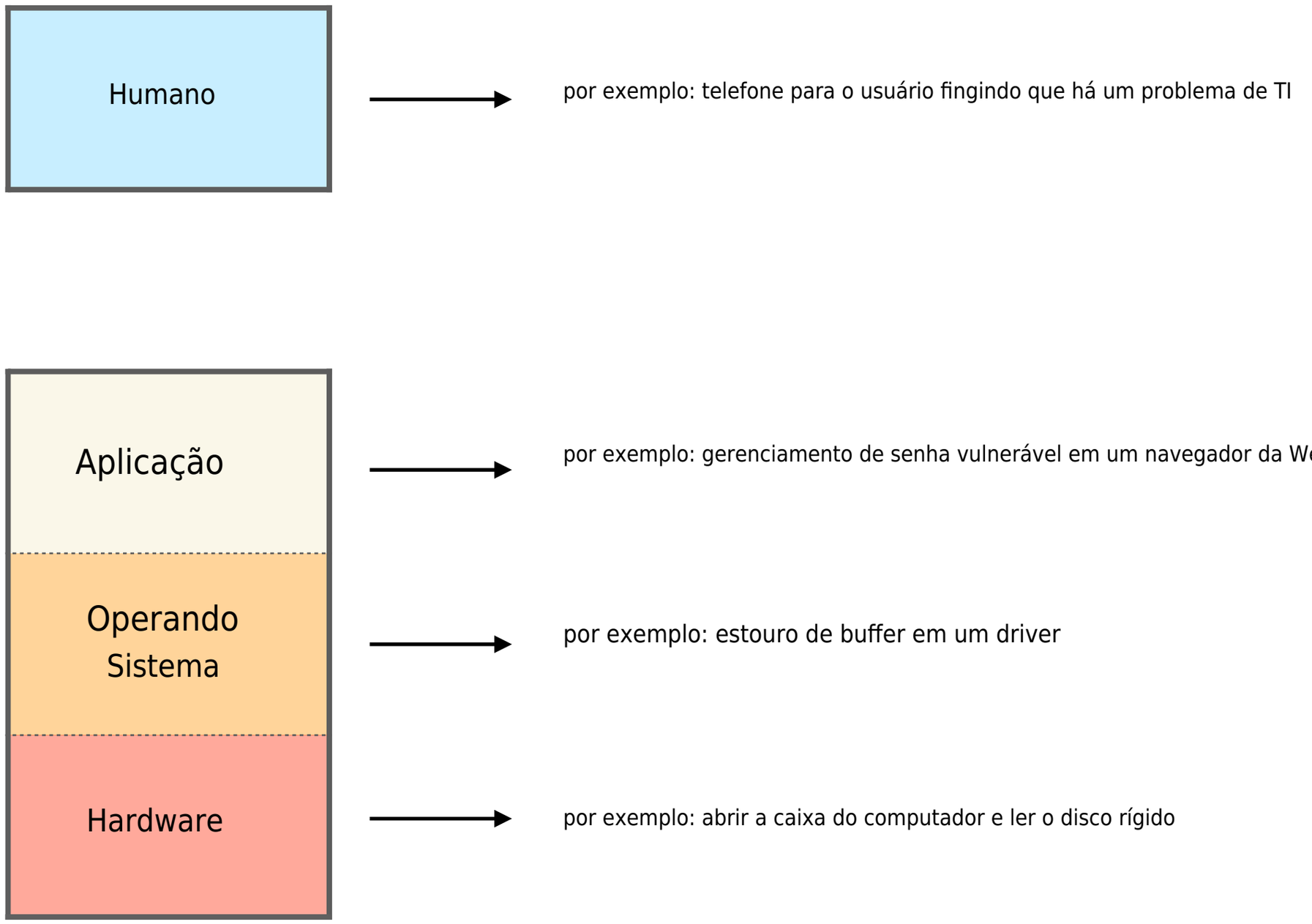
Atacante

- Ataquem solitário, criancinhas de script
  - geralmente executar ataques conhecidos através de explorações já disponíveis,...
- Criminosos profissionais/gangues
  - assumir o controle de milhares de computadores, SPAM, phishing, DDoS,...
- Governos
  - enorme poder informático, cripto-hacking, escutas telefónicas, poderes legais,...
- Provedor de serviços de Internet
  - fazer “espião” em você, pode vender (e soltar) seus dados,...
- Insiders
  - acesso a ativos, geralmente mais prejudiciais do que atacantes externos,...
- Outros: hacktivistas, vândalos, terroristas,...

Um exercício de modelo de ameaça

- Quais são as suas preocupações de segurança se você estiver:
  - um indivíduo
  - um grande negócio

Níveis de ataque



Segurança

- Segurança vs. Segurança
  - ação intencional versus ação não intencional não intencional: por exemplo, confiabilidade, problemas de usabilidade intencional: ação humana tenta explorar uma vulnerabilidade
  -

- Segurança vs. Confiabilidade
  - subconjunto de conceitos relacionados à dependência

Confiabilidade

Atributos
(propriedades)

- Confidencialidade
- Integridade
- Disponibilidade

Segurança
(acção intencional)

- Confiabilidade
- Usabilidade
- Manutenção

Segurança
(acção não intencional)

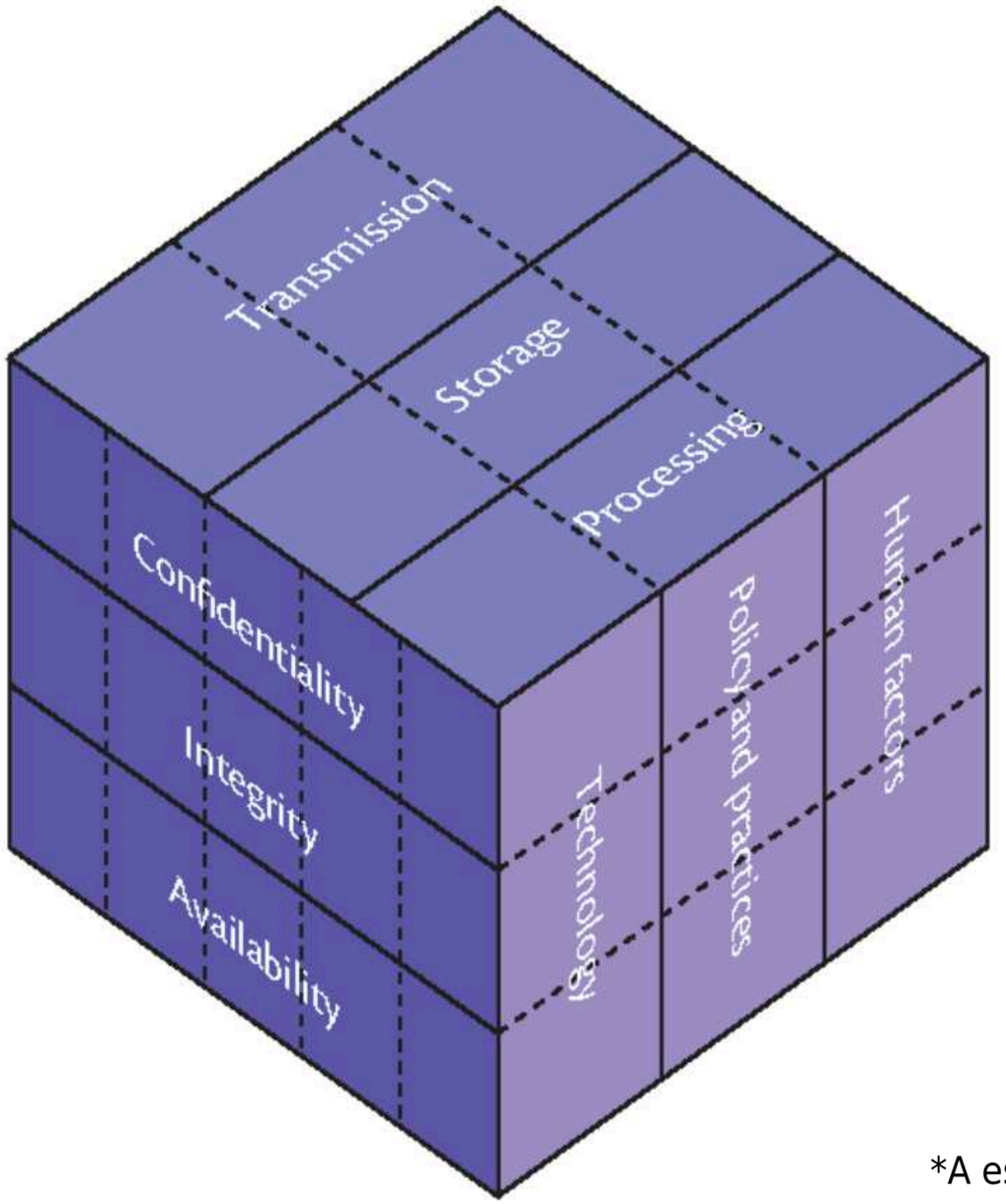
Ameaças
(emparelhamentos)

- Falhas
- Erros
- Fracassos

Meio
(medidas)

- Prevenção de falhas
- Tolerância a falhas
- Remoção de falhas
- Predição de falhas

Pensando em segurança*



*A estrutura McCumber

Segurança

	Configurações tradicionais	Sistemas de informações
Activo	Ouro	Informação
Objetivos	Não pode ser roubado	Confidencialidade Integridade Disponibilidade
Atacantes	Ladrões	Criminosos profissionais, governos, insiders,...
Proteção	Fechaduras, paredes, armadas guardas,...	Criptografia, protocolos, auditorias de segurança,...

Segurança

- Segurança como um “problema de pessoas”
    - não pode ser resolvido apenas pela tecnologia
- A segurança deve enredar
    - define um comportamento aceitável (por exemplo, proteção de dados e computador) uso indevido) define políticas e práticas dentro de uma organização, para cumprir com o direito geral e ser eficaz em fazer negócios as políticas e práticas organizativas devem traduzir-se em mecanismos de segurança posto em prática por peritos técnicos e sta ff todos os usuários devem cumprir as políticas e práticas da organização pensaram que o mecanismos de segurança implementados o sistema jurídico, a gestão da organização e os peritos técnicos devem colaborar a fim de alcançar uma segurança eficaz
    -
    -